

مركز البحوث والدراسات

أمن المعلومات
وإدارة مخاطر تقنية المعلومات

تأليف

مانيش أغروال

أليكس كامبو

إيرك بيرس

ترجمة

د. جعفر بن أحمد العلوان

راجع الترجمة

أ. د. عبدالله بن عبدالعزيز بن عبدالله التميم

بسم الله الرحمن الرحيم



مركز البحوث والدراسات

أمن المعلومات
وإدارة مخاطر تقنية المعلومات

تأليف

مانيش أغروال

أليكس كامبو

إيرك بيرس

ترجمة

د. جعفر بن أحمد العلوان

راجع الترجمة

أ. د. عبدالله بن عبدالعزيز بن عبدالله التميم

١٤٤٠هـ - ٢٠١٨م

بطاقة الفهرسة

ح معهد الإدارة العامة، ١٤٤٠هـ

فهرسة مكتبة الملك فهد الوطنية أثناء النشر

أغروال مانيش

أمن المعلومات وإدارة مخاطر تقنية المعلومات

مانيش أغروال؛ أليكس كامبو؛ إيرك بيرس؛ جعفر بن أحمد العلوان؛ عبدالله التميم.

الرياض، ١٤٤٠هـ

٧٨٤ ص؛ ١٧سم × ٢٤سم.

ردمك: ٢-٢٧٥-١٤-٩٩٦٠

١- أمن المعلومات ٢- أمن الحواسيب ٣- تقنية المعلومات

أ. كامبو، أليكس (مؤلف مشارك) ب. بيرس، إيرك (مؤلف مشارك)

ج- العلوان، جعفر بن أحمد (مترجم) د. التميم، عبدالله (مراجع)

هـ- العنوان

ديوي ٠٥٥,٨ ١٤٣٩/٧٦١١

رقم الإيداع: ١٤٣٩/٧٦١١

ردمك: ٢-٢٧٥-١٤-٩٩٦٠

هذه ترجمة لكتاب:

Information Security and IT Risk Management

First Edition

Manish Agrawal, Ph.D.
Information Systems and Decision Sciences
University of South Florida
Alex Campoe, CISSP
Director, Information Security
University of South Florida
Eric Pierce
Associate Director, Information Security
University of South Florida



٤

المحتويات

قائمة الأشكال

تمهيد:

تُعد المشــكلات التي تواجه طائر النمنمة الموجودة صورته على غلاف الكتاب مشكلات مصيرية تؤثر في حياة أو موت هذا الطائر، لكن مشكلات أمن المعلومات التي نواجهها نحن البشر ليســت كذلك (وللاطلاع على مشــكلة طائر النمنمة راجع ســؤال التفكير النقدي في الفصل التاســع). وعلى الرغم من ذلك فإن مشــكلات أمن المعلومات تُعد مزعجة ومُكْلِفة ومُســتمرة بما فيه الكفاية لتجعــل من أمن المعلومات مهنة العــصر الحديث وتجعل منه كذلك موضوعاً جديراً بالاهتمام والدراسة.

تم تصميم هذا الكتاب ليكون بمثابة مقرر دراسي مخصص لأمن المعلومات تتم دراسته خلال فصل دراسي واحد. ويركز الكتاب على مساعدة الطلاب في اكتساب المهارات المطلوبة في سوق العمل المهنية.

ويبــدأ هذا الكتاب بمقدمة عن البيئــة المهنية لأمن المعلومات. وبعــد اقتناع الطالب بأهميــة هذا الموضوع، يُقدّم الكتاب النموذج الأســاسي لأمن المعلومات والذي يتكون من الأصــول، والثغرات الأمنية، والتهديــدات، والضوابط. ونخصص ما تبقى من المقرر الدراسي لتوصيف الأصول، والثغرات الأمنية، والتهديدات والاســتجابة لها باستخدام التحكم الأمني. وينتهي هذا الكتاب بدمج هذه الموضوعات تحت المظلة العامة لإدارة المخاطر التنظيمية. وبنهاية المقرر الدراسي ســيكون لدى الطلاب الوعي بكيفية تطور الاهتمام بأمن المعلومات في مجتمعنا، وكيفية اســتخدام الأطر والنماذج الحديثــة للتعامل مع تلك المخاوف في بيئة احترافية.

وفي نهايــة كل فصــل من هذا الكتــاب هناك مجموعة كاملة مــن التمارين تتألف من خمسة أنواع من الأسئلة:

١. أسئلة تقليدية في نهاية كل فصل تهدف إلى تحسين فهم الطلاب واستذكار الموضوعات الهامة في أمن المعلومات.

٢. مثــال على حالة دراســية في نهاية كل فصل تتيح للطلاب تطبيــق المعارف التي تم اكتسابها في بيئة عملية.

٣. كـما تم تصميم حالة مترابطة بجميـع موضوعات فصول الكتاب. ويقوم الطالب في هذه الحالة المترابطة بدور مدير أمن المعلومات في إحدى الجامعات الحكومية حيث يواجه الطالب بعض المشكلات المتعلقة بالموضوعات التي تمت مناقشتها في الفصل.

٤. تمرين التفكير النقدي والذي يتعرف الطلاب من خلاله على حالات عملية مماثلة لما تم مناقشـته في الفصل حيث يقوم الطلاب بربط الأفكار من الفصل بهذه الحالات. وتُصنف المشـكلة التي تواجه طائر النمنمة والتي تم الإشـارة إليها آنفاً تحت هذا النوع من التمارين.

٥. وأخيراً يحتوي كل فصل على نشـاط عملي مُفصَّل باسـتخدام توزيع مخصص لنظام التشغيل سـنتوس لينكس (CentOS Linux OS) ليتم تثبيته بصفة جهاز افتراضي باسـتخدام (VirtualBox). ونحن فخورون جداً بهـذا الجانب من الكتاب. ولقد قمنا باختيار التمارين بعناية بحيث تسـاعد الطلاب ليصبحوا على معرفة بمهام أمن المعلومات الأولية من جهة وعلى معرفة أيضاً بإدارة بأنظمة لينكس من جهة أخرى. ولقـد قـام زميلنا إيرك على وجـه التحديد بقضاء وقت طويـل في اختبار وتصميم وصيانة التوزيع المخصص لنظام التشـغيل سنتوس لينكس (CentOS Linux OS). وبالإمكان تحميل هذا التوزيع من الموقع الإلكتروني للكتاب.

ومـع أن محتويات الكتاب بحـد ذاتها تُعد كافية دون الحاجة للأنشـطة العملية فقد تم إضافة محتوى النشـاط العملي اسـتجابةً لطلبات المسـؤولين في المنظمات. ونأمل من المدربـين أن يتيحوا لطلابهم الاسـتفادة من هـذا الجانب من الكتـاب. ويعرض الفصلان الثاني والثالث من هذا الكتاب الإعدادات الأساسـية لاسـتخدام الجهاز الافتراضي (Virtual Machine). وجـاءت التعليمات مفصلة بما فيه الكفاية حتـى يتمكن الطلاب من إكمال التمارين بمفردهم.

ويمكن الاسـتفادة من وقت المحاضرة بطرق شـتى عند الاسـتعانة بهذا الكتاب. مثلاً المحاضرات التقليدية ستكون ملائمة جداً مع هذا الكتاب. أما المدربون المهتمون بالاستفادة من الوقت في مزيد من الأنشـطة التفاعلية فسـيجدون أن الأنشطة والتمارين الموجودة في نهاية كل فصل ستكون طريقة مفيدة جداً للاستغلال الأمثل لوقت المحاضرة.

وقام فريق تأليف هذا الكتاب بدمج وجهات النظر المختلفة اللازمة لتدريس موضوعات أمـن المعلومات للارتقاء بالطموحات المهنيـة. المؤلف الأول هو مانيش أغروال وهو عضو هيئة تدريس متخصص في نظم المعلومات الإدارية. وقام بتصميم هذا المقرر الدراسي، كما قام بتدريسه لطلاب نظم المعلومات الإدارية والمحاسبة في جامعة جنوب فلوريدا لأكثر من خمس سـنوات حتـى الآن. المؤلف الثاني هو أليكس كامبو وهـو مدير أمن المعلومات في جامعة جنوب فلوريدا. وهو المتصدر لجميع أنشـطة أمن المعلومات في الجامعة متضمناً ذلك الاسـتجابة للحوادث ووضع السياسـات وتحقيق التوافق التقني. المؤلف الثالث هو إيرك بيرس وهو المسؤول عن إدارة الهوية في الجامعة. وترتكز الموضوعات التي تم تناولها في هذا الكتاب على معرفة فريق التأليف بأهم الأنشـطة اليومية التي تندرج تحت مظلة أمن المعلومات.

طائر النمنمة الذي سبق ذكره لا يواجه مشكلة أمن المعلومات على وجه التحديد لكنه يسـتخدم الحلـول التي تعتمد على كثـير من ضوابط أمن المعلومات التـي تُناقش في هذا الكتـاب؛ إذ يتضمن محيـط طائر النمنمة جميع مكونات نموذج أمن المعلومات الأسـاسي المُقترح في هذا الكتاب. فالأصول تتمثل في حياة صغار طائر النمنمة وسلالته، في حين تتمثل الثغرات في تأخر فقس البيض. أما التهديدات فهي الطيور الطفيلية، وأخيراً تتمثل الضوابط في رمـوز التعارف بين هذه الطيور. ومن ثم فإننا نعتقد بأن مشـكلة طائر النمنمة تصف هذا الكتاب بإيجاز.

ونود تأكيد حرصنا على سماع تعليقات القُراء عن الكتاب سواء كانت اقتراحات للتطوير، أم أخطـاء مطبعية، أو خلـلاً في الجهاز الافتراضي، أو أي موضوع آخـر يواجهه القُراء أثناء اسـتعراضهم لهذا الكتاب. وسوف نبذل قصارى جهدنا للاسـتجابة للمقترحات، وسنعرض التصحيحات في جدول للأخطاء المطبعية يوضح الخطأ والصواب وسنقوم بنشر هذا الجدول في الموقع الإلكتروني للكتاب. كما نود معرفة ملاحظات القُراء الإضافية المتعلقة بمدى قدرة الكتاب على تحسـين فهم موضوع أمن المعلومات، أو تطوير طريقة التدريس، أو المساعدة في الحصـول على وظيفة، أو المسـاعدة في العمل نفسـه. وستسـاعدنا هـذه التعليقات والملاحظات في تحسـين الطبعات المقبلة من الكتاب. ويُمكن إرسال التعليقات والملاحظات للمؤلف الأول على البريد الإلكتروني التالي: magrawal@usf.edu



الفصل الأول

المقدمة

نظرة عامة:

يُــبرِز هذا الفصــل أهمية موضوع أمــن المعلومات، كما يوضح أجــزاء ومكونات بقية هذا الكتاب. في البداية نذكر الأســباب التي تجعل من مجال أمن المعلومات مجالاً مفيداً للدراسة حتى نجعل القارئ متحمساً لموضوع هذا الكتاب. وبعد ذلك نقدم لمحة تاريخية عــن موضوع أمن المعلومات مع تســليط الضوء على أهم التطــورات التي أدت إلى الوضع الراهــن في مجال أمن المعلومات. وأخيراً ســنقوم بتلخيص الإجراءات المتبعة في مجال أمن المعلومات للحفاظ على أمن المعلومات. وهذه الإجراءات سنقوم بدراستها بالتفصيل خلال هذا الكتاب. في نهاية هذا الفصل يجب أن تعرف:

- الأسباب التي تجعل من موضوع أمن المعلومات موضوعاً مهماً لكل شخص في عصرنا الحاضر.
- أهم التطورات التي أدت إلى الوضع الراهن في مجال أمن المعلومات.
- المصطلحات الأساسية المستخدمة في أمن المعلومات.
- ملخص لإجراءات الحفاظ على أمن المعلومات.

الفوائد المهنية للمعرفة في مجال أمن المعلومات:

إذا كنــت تقــرأ هذا الكتــاب بوصفه جزءاً مــن متطلب جامعي فإنه عــلى الأرجح أن يُقدم هــذا المقرر الدراسي في كليات متخصصة ككلية إدارة الأعمال، أو نظم المعلومات، أو الهندســة. ومن المتوقع أن تقوم هذه الكليــات بتخريج الطلاب القادرين على بدء العمل الجديــد بحماس شــديد عند انضمامهم للقــوى العاملة. وبطبيعة الحــال فإننا نتوقع أن الســؤال الأســاسي في أذهان الطلاب في هذه الكليات هو: أين فرص العمل؟ وما الأهمية

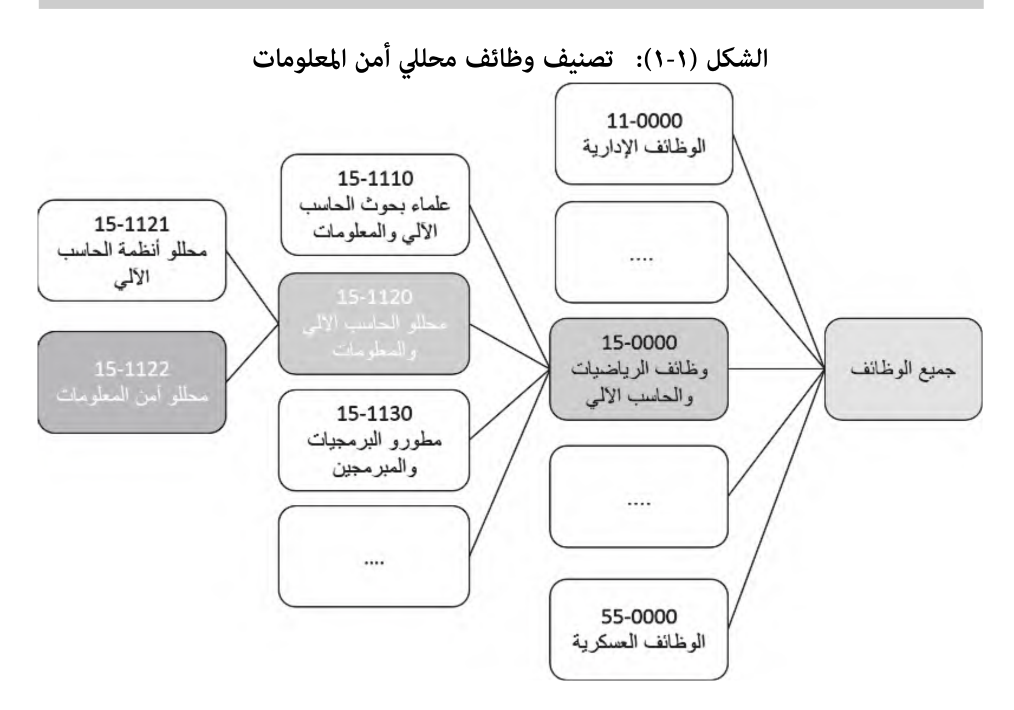
المهنيـة لموضـوع أمن المعلومـات؟ وما هو الطلـب الوظيفي عـلى المتخصصين في مجال أمـن المعلومات؟ وما الذي يدفع المنظـمات لتوظيف الخريجين من ذوي المهارات في أمن المعلومـات؟ وما الأعمال المتوقع أن يقوم الخريج بتنفيذها عند حصوله على وظيفة؟ وما الكفاءات التي تسـاعد الخريجين على تلبية تطلعات المسؤولين في المنظمات؟ قبل أن تقرر أن تقضي مزيداً من الوقت مع هذا الكتاب أو مع موضوع أمن المعلومات، نود أن نبدأ هذا الكتاب بالإجابة عن التساؤلات السابقة.

تقديرات الطلب:

يُعد مكتب إحصاءات العمل المصدر الأسـاسي لتقديـرات التوظيف في الولايات المتحدة الأمريكية[1]. و(مكتب إحصـاءات العمل) هو جهة حكومية تجمع إحصاءات التوظيف من دراسات مسحية واسعة لأرباب العمل. وقد قام هذا المكتب بتصميم تصنيف يسمى معيار التصنيف المهني القياسي standard occupational classification (SOC) لجميع الفئات المهنية الرئيسـية. وقد أعطي محللو أمن المعلومات الرمز ٢٢-١١-١٥ (شـكل ١-١). وتقع وظائف محللي أمن المعلومات تحت مجموعة وظائف الرياضيات والحاسب الآلي الرئيسية التـي تحمل الرمز (٠٠٠٠-١٥). ويشـير الموقع الإلكتروني لمكتـب إحصاءات العمل إلى أن إحصـاءات التوظيف الخاصة بمحللي أمن المعلومات قـد جُمعَت مع إحصاءات التوظيف الخاصة بمطوري صفحات الشبكة ومهندسي شبكات الحاسب الآلي. وبلغ إجمالي الوظائف في شـهر مايو من عام ٢٠١٠ لهذه المجموعة ٢٤٣٣٣٠ بمتوسـط راتب سنوي قدره ٧٩٣٧٠ دولاراً أمريكياً.

(1) http://www.bls.gov/

الشكل (١-١): تصنيف وظائف محللي أمن المعلومات



وتُعد الشهادات المهنية التي تصدرها المنظمات المهتمة بمجال أمن المعلومات من أبرز مصادر توقع طلب المنظمات لوظائف أمن المعلومات. وأحد هذه المنظمات الرائدة هي الاتحاد الدولي لشهادات أمن نظم المعلومات International Information System Security Certification Consortium (ISC) [٢] واستناداً إلى دراسة مسحية لأكثر من ١٠٠٠٠ موظف أمن معلومات من جميع أنحاء العالم، قدرت منظمة (ISC) في عام ٢٠١٠ أن هناك ما يقارب من ٢,٢٨ مليون موظف أمن معلومات في جميع أنحاء العالم منهم ٩٠٠٠٠٠ في القارتين الأمريكيتَين. ويُقدر أيضاً أن ينمو هذا الرقم بأكثر من ١٣٪[٣]. كما يُقدر متوسط المكافآت السنوية بأكثر من ٧٨٠٠٠ دولار أمريكي. ويُمكن أن يُعزى الفرق الواسع في تقديرات التوظيف بين الدراستين المسحيتين إلى اختلاف خصائص المنظمات المشمولة في كل دراسة. كما تجدر الإشارة إلى أن كلا الدراستين المسحيتين تتفقان تماماً في تقديراتهما لمتوسط المكافآت السنوية.

(2) http://www.bls.gov/oes/current/oes151179.htm

(3) https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf

دوافع الطلب الوظيفي على وظائف أمن المعلومات:

هناك العديد من العوامل التي تؤثر في طلب وظائف أمن المعلومات. أول هذه العوامل هو الأهمية المتزايدة للمعلومات لكل من الأفراد والمنظمات. إضافة إلى ذلك الزيادة الكبيرة في كمية المعلومات التي تقوم المنظمات بجمعها وتخزينها في أنظمة الحاسب الآلي بهدف استردادها والرجوع إليها. إن حيازة لص على بيانات الدخول على نظام ما (اسم المستخدم وكلمة المرور) قد تكون أثمن بالنسبة لهذا اللص من امتلاك ١٠٠ دولار أمريكي. وقد تسفر الهجمات الناجحة على أحد البنوك أو المؤسسات التجارية عن تسرب مئات الألوف من أسماء المستخدمين وكلمات المرور الموثقة. لذا فإن لدى كثير من المجرمين دافع ورغبة أكبر في استهداف مخازن المعلومات بدلاً من المخازن المادية الأخرى.

وعلى الرغم من أن المعلومات أصبحت أكثر قيمة فإن كثيراً من المستخدمين، ومن غير قصد، جعل من السهل على المهاجمين الحصول على هذه المعلومات القيمة. على سبيل المثال عندما يتطلب الأمر على المستخدمين تكوين اسم مستخدم وكلمة مرور فإن كثيراً منهم يعمد إلى استخدام رموز قصيرة في تكوين اسم المستخدم وكلمة المرور. كما أنهم غالباً ما يفضلون أن يقوم جهاز الحاسب الآلي بتذكر اسم المستخدم وكلمة المرور بدلاً من إدخالها في المواقع الإلكترونية التي يرتادونها. تأمل الآن فيما يحدث في حال تمكن المهاجم من وضع يده على جهاز الحاسب الآلي المحمول أو الجهاز اللوحي أو الهاتف الذكي الخاص بمستخدم ما. بدون أدنى شك أن هذا المهاجم سيتمكن من حيازة الكثير من المعلومات الحساسة عن هذا المستخدم. يستطيع المهاجم بسهولة وبأقل جهد الحصول على مئات الآلاف من بيانات المستخدمين. وتُوظِّف المنظمات ملايين الموظفين الذين يتعاملون بشكل مباشر مع بيانات المنظمات الحساسة. وفي الوقت ذاته يقوم هؤلاء الموظفون أثناء عملهم باستخدام أجهزتهم الذكية التي يُقدر عددها بالمليارات. لذا فإن المنظمات تضطر للعمل بشكل استباقي لتجنب الظهور على الصفحات الأولى للصحف والقنوات التلفزيونية بسبب فقدانها معلومات العملاء أو غيرها من البيانات الحساسة.

أهمية المعلومات الموضحة أعلاه هي أحد دوافع الطلب الوظيفي على وظائف أمن المعلومات. أما الدوافع الأخرى للطلب الوظيفي على وظائف أمن المعلومات فتشمل:

التعامـل مع ثغرات التطبيقات الحاسـوبية، والتيار المسـتمر من الفيروسـات والبرمجيات الخبيثة الأخرى التي تصـل للمنظمات، واللوائح التنظيمية، وخصوصية العملاء وتوقعاتهم بهذا الشأن، والموظفون المُستاؤون.

كـما أن دوافـع الطلب الوظيفي على وظائف أمن المعلومات قد تغيرت بشـكل سريع جداً. على سبيل المثال، حتى عام ٢٠٠٨ لم تكن الأجهزة المحمولة كالهواتف الذكية والأجهزة اللوحية أمراً مألوفاً في المنظمات. وبدلاً من ذلك كانت الهواتف الصادرة من المنظمة مصدر اعتزاز وفخر لدى المديرين التنفيذيين. وبحلول عام ٢٠١٠ أصبح معظم الموظفين يفضلون اسـتخدام هواتفهم الذكية الشـخصية وأجهزتهم اللوحية لإنجاز أعـمال المنظمة بدلاً من الهواتف التي تصدرها المنظمة والتي لا تحتوي في الغالب على متصفح الشبكة وغيرها من المميزات المرغوب فيها. ومن هنا وجب على موظفي أمن المعلومات أن يسـارعوا للتعامل مع الآثار البعيدة المدى لهذا التغيير. وبينما كانت المنظمات في وقت سابق تصدر الهواتف، مثل هاتف بلاكبيري، وتفرض السياسـات الأمنية المطلوبة على الأجهزة، أصبحت السياسات الأمنية للأجهزة الشـخصية تحت سيطرة المستخدمين وليست تحت سيطرة المنظمات التي يعملـون فيها. ونتيجة لذلك أفـاد موظفو أمن المعلومات في عـام ٢٠١٠ أن أمن الأجهزة المحمولـة والتعامل معها يـأتي على رأس أولوياتهم. ومن المرجـح أن تزداد هذه المخاوف في المسـتقبل القريب. ونتيجة لذلك فإن الطلب على وظائف أمن المعلومات وتأمين فرص وظيفية للعاملين في هذا المجال سيزداد أيضاً.

الأنشطة الوظيفية لموظفي أمن المعلومات:

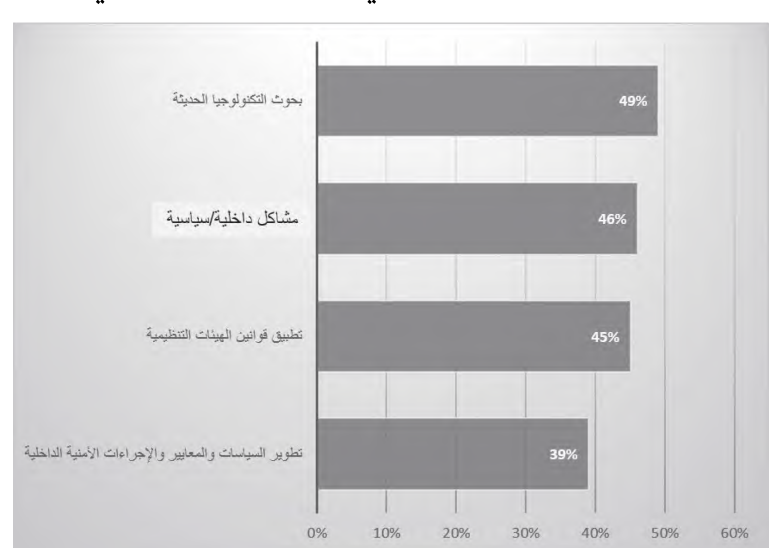
ما الأنشـطة التي يقـوم بها موظفو أمن المعلومات؟ حسـب الموقع الإلكتروني لمكتب إحصاءات العمل فإن دور محللي أمن المعلومات يتجسد فيما يلي:

تخطيط وتنفيذ وتطوير ومراقبة الإجراءات الأمنية المرتبطة بحماية شـبكات الحاسـب الآلي والمعلومـات. وتتضمن المهام التأكد من اسـتخدام الضوابط الأمنية المناسـبة لحماية الملفات الرقمية والبنية التحتية الإلكترونية. كما تتضمن المهام الاستجابة الفورية للفيروسات والخروقات الأمنية لأجهزة الحاسب الآلي.

أمثلة توضيحية: أخصائي أمن حاسب آلي، محلل أمن شبكات، أخصائي أمن الإنترنت.

وهذه الأنشــطة كلها إلى حد ما أنشطة تقنية. ومع ذلك فإن هناك الكثير من الأنشطة غير التقنية بطبيعتها والتي يقوم بها موظفو أمن المعلومات. ويوضح الشكل (١-٢) المراكز الأربعة الأولى للأنشــطة التي تستغرق وقتاً طويلاً حســب المشاركين في الدراسة المسحية[٤] والمعــدة من قبل منظمة ISC2. ومن هذا الشــكل يتضــح أن القضايا التنظيمية، وتطوير السياسات، والقضايا الإدارية تشكل الجزء الأكبر من أنشطة أمن المعلومات.

الشكل (١-٢): المراكز الأربعة الأولى للأنشطة التي تستغرق وقتاً طويلاً لموظفي أمن المعلومات



الكفاءات المطلوبة:

المسؤولية الرئيسية لموظفي أمن المعلومات تتمثل في تنبؤ المشكلات المتعلقة بالمعلومات والتقليل من آثار تلك المشــكلات. وتسلط الدراسة المسحية المعدة من قبل منظمة ISC2 الضوء على ثمان موضوعات تدريبيــة لموظفي أمن المعلومات. وهذه الموضوعات الثمانية موضحة في الشــكل (١-٣). وتُعد هذا الموضوعات الثمانية مؤشراً جيداً للكفاءات المطلوبة في المجال الوظيفي لأمن المعلومات. وبناءً على ذلك نســتطيع أن نرى بوضوح أن موظف أمن المعلومــات الناجح يحتاج إلى مهارة عالية في تحليل النظــم وتصميمها وذلك لتحديد

(4) https://www.isc2.org/uploadedFiles/Landing_Pages/NO_form/2011GISWS.pdf

الثغرات المحتملة التي قد تُصيب التطبيقات الإلكترونية للمنظمة. كما يحتاج موظف أمن المعلومـات الناجـح إلى مهارات في إدارة النُظم وذلك لاختبـار الأنظمة وتحديد الآثار التي يتركهـا قراصنة الإنترنت (الأدلة الجنائية). ويحتاج موظف أمن المعلومات الناجح أيضاً إلى مهارات في إدارة المخاطر. إن اسـتمرارية العمل من جهة ومتطلبات التعامل مع الكوارث مـن جهة أخرى يُحتم على موظفي أمن المعلومات أن يكون لديهم فهم جيد لطبيعة عمل المنظمـة بالإضافـة إلى فهمهم في بنيتهـا التحتية التقنية، وذلك لتحديـد التطبيقات الأكثر أهميـة للمنظمة من أجل اسـتعادة هذه التطبيقات سريعاً والتأكد من اتصالها بالشـبكة وذلك في حال كوارث طبيعية أو متعمدة.

الشكل (١-٣): الاحتياجات التدريبية لموظفي أمن المعلومات



ويهـدف هذا القسـم لإقناع القارئ بـأن وظائف أمن المعلومات هـي وظائف حيوية وعمليـة. كما يهدف إلى إيصال فكرة أن وظائف أمن المعلومات هي وظائف مُحفزة جداً. وعلاوة على ذلك فإن ثغرات أمن المعلومات تجذب مراقبة الجمهور مما يجعل من أنشطة موظفي أمن المعلومات ذات أهمية كبيرة للإدارة العليا في المنظمة ربما أكثر من بقية أجزاء البنية التحتية التقنية للمنظمة. في الوقع، وحسـب الدراسـة المسـحية٤ المعدة من قبل

منظمـة ISC2 فإن موظفي أمن المعلومـات يرفعون تقاريرهـم إلى الإدارة العليا كالمدير التنفيـذي للمنظمـة (CEO) أو المدير التنفيذي للمعلومـات (CIO) أو إلى مدير آخر في المستوى التنظيمي نفسه، وذلك في أكثر من (٢٥٪) من المنظمات.

لمحة تاريخية:

من هذا القسـم وما يليه نسـتطيع افتراض أن القارئ مهتم بتعلم أمن المعلومات من منظـور مهني. بمعنى أن القارئ مهتم بالاسـتفادة من موضوعات هـذا الكتاب في حياته المهنية. وتجدر الإشـارة إلى أن معظم الأشـياء التي نفعلها بشأن أمن المعلومات في عصرنا الحديث هي نتاج لتفاعل صناعة أمن المعلومات مع الثغرات الأمنية الشـهيرة التي حدثت على مر السـنين. وأصبحت العديد من هذه الحـوادث التاريخية جزءاً من التاريخ المهني لأمن المعلومات. إنه من المفيد بالنسـبة للقـارئ أن يتعرف على هذه الحوادث التاريخية حتى يدرك أهمية المتطلبات التنظيمية، ويُقدر مخاوف المديرين، ويتعرف على المصطلحات المهنيـة الخاصة بأمن المعلومات. وتحتوي القائمة أدناه على بعض حوادث أمن المعلومات التاريخيـة. وليس الهدف من هذه القائمة أن تكون شـاملة لجميع الحوادث التي حدثت في المـاضي[٥]، بـل الهدف منها هو التركيز على حوادث أمن المعلومات الرئيسـية التي أدت إلى اعتماد الإجراءات التنظيمية وإلى تفاعل صناعة أمن المعلومات ولكونها مقياساً لمخاوف أمن المعلومات التي حدثت في ذلك الوقت.

١٩٨١- تطويـر تقنيات الإنترنت الرئيسـية (TCP and IP): تـم الانتهاء من التقنيات الأساسـية للإنترنـت في عام ١٩٨١ ولم يكن هناك أي ذكر لمسـألة أمـن المعلومات في هذه التقنيات مما يُشير إلى أن عالم التكنولوجيا لم يكن يشعر بالقلق إزاء أمن المعلومات في ذلك الوقت. وكانت تقنيات الإنترنت الرئيسية (TCP and IP) متاحة مجاناً، ومن ثم أصبحت هذه التقنيات هي تكنولوجيا الشبكات المفضلة لأنظمة الينكس (UNIX) والتي تُستخدم بشكل واسع في الجامعات والمنظمات المختلفة كالمستشفيات والبنوك.

١٩٨٢-١٩٨٣-عصابة ٤١٤: بدأت عمليات الاقتحام الإلكتروني بعد وقت قصير من دمج تقنيات الإنترنت الرئيسـية (TCP and IP) بمعدات وتجهيزات قطاعات الأعمال المختلفة . وكان حادث عصابة ٤١٤ هو الحادث الأكثر تغطية إعلامية في ذلك الوقت. وتتكون العصابة

(٥) لمصدر أكثر شمولاً على الموقع التالي: Wikipedia: http://en.wikipedia.org/wiki/Timeline_of_computer_security_hacker_history

من ستة من المراهقين من مدينة ميلووكي، وسُميت العصابة بالرمز الهاتفي لمنطقة ميلووكي وهـو ٤١٤. ووجد هـؤلاء المراهقين أنه من المثير الوصول إلى الأنظمة التي من المفترض أن تكون بعيـدة عن متناول أيديهم. وتمكنت هذه المجموعة من اقتحام ما يقارب ٦٠ نظاماً حاسوبياً رفيع المسـتوى باستخدام أجهزة الحاسب الآلي وخطوط الهواتف المنزلية وكلمات مـرور افتراضية. ومـن المنظمات التي تم اقتحامها من قبل هـذه العصابة مختبرات لوس ألاموس ومركز ميموريال سـلون كيترينج للسرطان في نيويورك. وتلقى هذا الحادث تغطية واسعة من وسائل الإعلام متضمناً ذلك الصفحة الأولى لمجلة نيوزويك والتي تضمنت العنوان التـالي (احترس: قراصنة الحاسـب يعبثـون). ويُعتقد أن هذا هو أول اسـتخدام لمصطلح قراصنة الحاسـب في وسـائل الإعلام في سـياق أمن الحاسـب الآلي. وفي حين أن المراهقين لم يُحدثـوا أي ضرر، رأى القائمـون على الأنظمة في ذلك الوقت أن التقنيات البسـيطة التي يسـتخدمها الأطفال من السـهل تكرارها من قبل الآخرين. ونتيجة لذلك عقد الكونغرس الأمريكي جلسـات اسـتماع حول أمن الحاسـب الآلي. وبعد المزيد من مثل هذه الحوادث أصدر الكونغرس قانون الاحتيال وإسـاءة استخدام الحاسب الآلي عام ١٩٨٦. ويجعل هذا القانون من اقتحام أنظمة الحاسب الآلي الحكومية أو الخاصة جريمة يعاقب عليها القانون.

١٩٨٨- دودة موريس الخبيثة: درس روبرت موريس الدراسـات عليا في جامعة كورنيل وهو حالياً بروفسـور في علوم الحاسـب الآلي والذكاء الاصطناعي في معهد ماساتشوسـتس للتكنولوجيا (MIT). وفي الثاني من نوفمبر من عام ١٩٨٨ أصدر موريس برنامجاً حاسـوبياً لتكرار ٩٩ خطاً تكرارياً ذاتياً، وذلك لقياس حجم الإنترنت الحديثة المنشأ. ونتيجة لمميزات تصميم البرنامج تعطل العديد من أنظمة الحاسب الآلي. كما نتج عن هذه العملية العديد من الأحداث وذلك لأن هذا البرنامج يُعد أول دودة خبيثة للإنترنت. وتشـير الأرقام إلى أن هذه الدودة عطلت ما نسبته (١٠٪) من الإنترنت وهو أكبر جزء يُعطل من الإنترنت على مر التاريخ وحتى عصرنا الحالي. كما أسفر هذا الحادث عن أول إدانة بموجب قانون الاحتيال وإسـاءة استخدام الحاسـب الآلي لعام ١٩٨٦. وحُكم على روبريت موريس بالوضع تحت الرقابـة، وخدمة المجتمع، ودفع غرامة مالية. كما دفعت هـذه الحادثة حكومة الولايات المتحدة الأمريكية إلى إنشـاء فريق اسـتجابة لطوارئ الحاسـب الآلي (CERT/CC)[٦] في جامعـة كارنيجي ميلون (CMU) ليكون مركزاً لتنسـيق تفاعـل الحكومة وقطاع الأعمال

(٦) يقصد بـ (CERT) فريق استجابة لطوارئ الحاسب الآلي. كما تم تسجيل (CMU) كعلامة تجارية في مكتب براءة الاختراع والعلامات التجارية الأمريكي.

لحوادث الإنترنت المشـــابهة. وتجدر الإشـــارة إلى أن البروفســـور روبرت موريس كان أحد المؤسســـين لموقع Viaweb وهـــو أحد شركات التجارة الإلكترونيـــة والتي قامت شركة ياهو بشرائها وإعادة تسميتها إلى (Yahoo! Store).

ومن الظريف والمثير للاهتمام أن والد روبرت موريس هو بوب موريس وهو الشخص الذي قام بتصميم نظام تشـــفير كلمة المرور لنظام التشغيل ينكس UNIX والذي يُستخدم حتى يومنا الحالي. ومـــا يثير الاهتمام أكثر أن بـــوب موريس في وقت هذه الحادثة كان أحد كبـــار العلماء في مركز أمن الحاســـب الآلي الوطنـــي (NCSC) التابع لوكالة الأمن القومـــي (NSA)[(٧)، (٨)] وهي الوكالة الاتحادية المسؤولة عن تصميم أجهزة الحاسب الآلي الآمنة.

١٩٩٥-١٩٩٨- نظام ويندوز ٩٨/٩٥: أصدرت مايكروســـوفت نظام التشـــغيل (ويندوز ٩٥) في الرابـــع والعشريـــن من أغســـطس من عـــام ١٩٩٥. وكان يحتوي هـــذا النظام على واجهة مستخدم رسومية، كما كان هذا النظام مصمماً ليعمل على أجهزة غير مُكلفة نسبياً. وعنـــد طرحٍ هذا الإصدار في الســـوق تم دعمه بحملة تســـويقية كبـــيرة، وخلال فترة زمنية قصيرة جداً أصبح ويندوز ٩٥ نظام التشـــغيل الأكثر نجاحاً على الإطلاق مما أدى إلى خروج أنظمة التشـــغيل الأخرى من الســـوق. وفي المقام الأول تم تصميم ويندوز ٩٥ ليكون نظام تشـــغيل مســـتقلاً لمســـتخدم واحد ومن ثم لم يكن يحتوي على أي احتياطات أمنية. وكان معظم المســـتخدمين يعملون على النظام دون كلمة مرور، وكانت معظم التطبيقات تعمل بامتيازات مدير الحســـاب، وذلك لتوفير الوقت والجهد على المســـتخدمين. ومع ذلك فإن نظام ويندوز ٩٥ يدعم تقنيات الإنترنت الرئيسية (TCP/IP) والذي أدى إلى استخدام هذه التقنيات من قِبل معظم شركات الأعمال. هذا المزيج بين تقنية شـــبكات لا تعتمد على أي احتياطات أمنيَة كتقنية (TCP/IP) وبين بيئة عمل لا تعتمد أيضاً على أي احتياطات أمنية خلـــق بيئة خصبة ومزدهرة للتنازل عن أولويات أمن المعلومات. ويشـــير خبراء المعلومات في محادثاتهـــم أحياناً إلى أن هذه البيئة هي مصدر وظائف أمن المعلومات[(٩)]. وحتى نظام التشغيل (ويندوز ٩٨) والذي صدر في الخامس والعشرين من يونيو من عام ١٩٩٨ لم يحتوِ على أي تعديل في أساسيات التصميم الأمني للنظام.

(7) http://cm.bell-labs.com/cm/cs/who/dmr/crypt.html

(٨) ولمعلومات أكثر إثارة عن بوب موريس يمكن قراءة الكتاب الهزلي التالي من تأليف كليف ستول, "The Cuckoo›s Egg," ISBN 0671726889.

(٩) على سبيل المثال أشار دان الجير، وهو ضابط أمن المعلومات في (In-Q-Tel) أحد الأذرع الاستثمارية لوكالات المخابرات الأمريكية، إلى ذلك في حديثه في اجتماع (ISSA) في تامبا في ديسمبر من عام ٢٠١١.

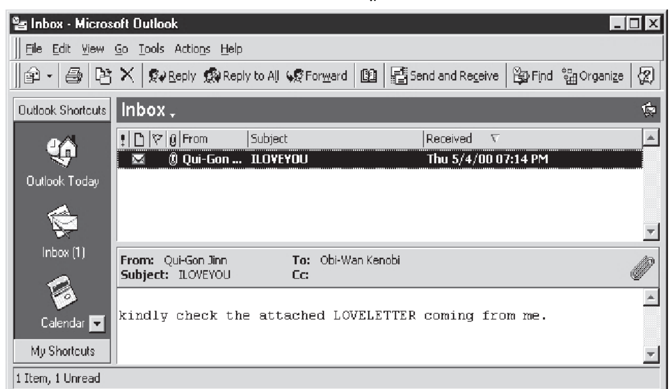
١٩٩٦- قانون إمكانية نقل التأمين الصحي والمساءلة Health Insurance Portability and Accountability Act (HIPP): هــذا القانــون يركــز في المقــام الأول على حماية التأمين الصحي للعاملين في الولايات المتحدة الأمريكية عند تغيير أو فقدان وظائفهم. ولهذا القانــون آثار أيضاً عــلى أمن المعلومات حيث كان العديد من قــادة الأجهزة الحكومية في ذلك الوقت يعتقد بأهمية الســجلات الصحية الإلكترونية (EHR) لتقليل تكاليف الرعاية الصحية المرتفعة في أمريكا. ومن ثم جاء هذا القانون ليدفع باتجاه تبني السجلات الصحية الإلكترونيــة. وبما أن موضوع أمن المعلومات من الموضوعــات التي حظيت باهتمام كبير، احتــوى هذا القانون عــلى بنود وأحكام تجعل المنظمات مســؤولة عن الحفاظ على سرية ســجلات المرضى في قطاع الرعايــة الصحية. وفي الوقت الحالي يتوجــب على قطاع الرعاية الصحيــة التحــول إلى الســجلات الصحية الإلكترونية بحلــول عام ٢٠١٤. وهــذا هو أحد المحركات الرئيســية للطلــب على أمن المعلومات حتى وقت كتابة هذه النســخة من هذا الكتاب (٢٠١٢-٢٠١٣).

٢٠٠٠- فيروس ILOVEYOU: أصدر طالبان من الفلبين هذا الفيروس في الخامس من مايو من عام ٢٠٠٠ (الشــكل ١-٤). ويقوم هــذا الفيروس بحذف جميع الصور من أجهزة الحاســب الآلي المصابة. كما يقوم بإرسال نفســه تلقائياً كملف مرفق إلى قائمة الاتصال في برنامج أوتلوك. وأصاب هذا الفيروس الملايين من أجهزة الحاسب الآلي، كما تسبب بخسارة مليــارات الدولارات. وتمكنت الحكومــة الأمريكية من تتبع من قام بتصميم هذا الفيروس في غضون ســاعات من إطلاقــه وهما الطالبان روميل راموزز، وونيــل دي جوزمان. ولكن المحققــين أدركوا بسرعة أنه لا يوجد قانون ضد إصدار الفيروســات الحاســوبية في الفلبين. وتوجب على المحققين في هذه الحالة إســقاط جميع التهم الموجهة للطالبين[١٠]. وقد أدت هذه الحادثة إلى إدراك أن أمن المعلومات ظاهرة عالمية مما ولد ضغطاً من الدول المتقدمة عــلى الدول النامية لتطوير وإصلاح قوانين أمــن المعلومات الخاصة بهم. ومع ذلك ما زال هناك اختلاف كبير بين الدول فيما يتعلق بقوانين أمن المعلومات. على سبيل المثال، إصدار فيروس حاسوبي في الولايات المتحدة الأمريكية قد يؤدي إلى غرامة مالية تصل إلى ٢٥٠,٠٠٠

(10) Arnold, W. “TECHNOLOGY: Philippines to drop charges on e-mail virus,” New York Times, August 22, 2000.

دولار أمريكي و١٠ أعوام سجن. أما العقوبة في الفلبين فتتراوح بين ١٠٠,٠٠٠ بيزو (٢٥٠٠ دولار أمريكي) ومبلغ يتناسب مع الأضرار بالإضافة إلى ٣ أعوام سجن[١١].

الشكل (١-٤): فيروس ILOVEYOU



٢٠٠٢- قانون ساربينز أوكسلي (Sarbanes-Oxley Act):

خلال الفترة من عام ٢٠٠٠ إلى عام ٢٠٠٢ شهدت الولايات المتحدة الأمريكية حالات مزعجة لاحتيال بعض الشركات الكبيرة كشركة أنرون، وتايكو، و وورلدكوم. ادعت شركة أنرون في عام ٢٠٠٠، على سبيل المثال، إيرادات بأكثر من ١٠٠ مليار دولار أمريكي لكنها أعلنت إفلاسها في العام التالي. في مثال آخر بالغت شركة وورلدكوم في تقدير أرباحها لعام ٢٠٠٢ بأكثر من ٧٢ مليار دولار أمريكي خلال ١٥ شهراً. ويُعتقد أن هذه الاحتيالات قد تمت من خلال التلاعب بالأنظمة المحاسبية بأمر من قيادة المنظمة. لكن وخلال المحاكمات كان المديرون التنفيذيون يحاولون باستمرار الهرب من المسؤولية بادعاء جهل الإجراءات المحاسبية وإلقاء اللوم على ثقتهم العمياء في مساعديهم ذوي التعليم العالي والرواتب الممتازة. وأثّر سقوط هذه الشركات على معظم العوائل الأمريكية لأن رواتبهم التقاعدية يتم استثمارها في الشركات الكبيرة المطروحة للتداول العام. ووجد الكونغرس الأمريكي نفسه مضطراً للتصرف لضمان سلامة التقارير المالية حيث أصدر الكونغرس قانون ساربينز أوكسلي (Sarbanes-Oxley Act) في عام ٢٠٠٢. وركز القانون على جعل المسؤولين

(11) http://www.chanrobles.com/ecommerceimplementingrules.htm (accessed 02/28/2012)

التنفيذيين مسؤولين شخصياً عن صحة التقارير المالية للشركات المطروحة للتداول العام. ويتضمن هذا القانون ثلاثة أقسام. قسم ٣٠٢ من هذا القانون يتطلب أن يقوم المدير التنفيذي والمدير المالي بالتوقيع على إقرار بمعرفتهم الشخصية بكل المعلومات الواردة في التقارير السنوية. كما يفرض قسم ٩٠٦ من القانون عقوبات جنائية متضمناً ذلك السجن لمدة تصل إلى ٢٠ سنة لأي إقرارات غير صحيحة. أما القسم الذي له تأثير مباشر في أمن المعلومات ووظائفها فهو قسم ٤٠٤، لأن هذا القسم يتطلب أن يكون الإقرار في قسم ٣٠٢ معتمداً على أسس رقابة داخلية رسمية. وقد أدى ذلك إلى استثمارات كبيرة في الرقابة الداخلية على التقارير المالية للشركات المطروحة للتداول العام.

٢٠٠٥-٢٠٠٧ الهجمات الإلكترونية على شركات التجزئة: في ديسمبر من عام ٢٠٠٦ ذكرت شركة تي جي ماكس (T.J.Maxx) أن أنظمتها الحاسوبية والتي تتضمن بطاقات الدفع الائتمانية تم اختراقها (الشكل ١-٥). وتبين من التحقيقات أن الاختراق بدأ قبل عام ونصف وبالتحديد في يوليو من عام ٢٠٠٥ وتم سرقة بيانات أكثر من ٤٥ مليون بطاقة ائتمانية. واتضح أن قائد المجموعة المتورطة في عملية الاختراق يدعى ألبرت غونزاليس وهو موظف في مخابرات جهاز الخدمة السرية الأمريكية. وفي واقع الأمر كان ألبرت في وقت الهجمات يتواصل مع جهاز الخدمة السرية بخصوص حالة أخرى. وكشفت التحقيقات أيضاً أن هذه المجموعة قد قامت باختراق الأنظمة الحاسوبية في العديد من شركات التجزئة مثل (BJ›s Wholesale Club, DSW, Office Max, Boston Market, Barnes & Noble, and Sports Authority). وكانت طريقة عمل المجموعة كالتالي: أولاً قيادة السيارة على الطريق السريع رقم ١ في ميامي، ومن ثم البحث عن شركة للتجزئة شبكتها اللاسلكية غير مؤمنة بشكل جيد، وبعد ذلك يتم الدخول على شبكة الشركة. وفي وقت لاحق قامت المجموعة بتطوير طريقة عملها وذلك باستخدام حقن تعليمات الاستعلام البُنيوية (SQL injection) للدخول للشبكة الحاسوبية لشركة (Hannaford Brothers and Heartland Payment Systems) وهي الشركة المسؤولة عن التعامل مع بطاقات الدفع الائتمانية. وبحسب بعض التقديرات فإن بيانات أكثر من ١٢٥ مليون بطاقة ائتمان تم سرقتها من هذه الشركة. كما تقدر الشركة خسائرها بأكثر من ١٢ مليون دولار أمريكي. وفي مارس من عام ٢٠١٠ تم الحكم على ألبرت غونزاليس بالسجن ٢٠ سنة، كما تم تغريمه

أكـثر من ١,٦٥٠,٠٠٠ دولار أمريكي والتي حصـل عليها من بيع البطاقات المزيفة. وأبرزت هـذه الحوادث أنه حتى الشركات الكبيرة لديها ضعف واضح فيما يتعلق بأمن المعلومات، ويمكـن أن يؤدي هـذا الضعف إلى الكثير من الإرباك والخسـائر المالية الكبيرة. وقد أدى اسـتخدام تقنية حقن تعليمات الاسـتعلام البنيوية (SQL injection) على وجه الخصوص إلى تأسيس الوعي للاهتمام بأمن المعلومات من خلال تطوير البرمجيات. ومن هذا الوعي نشـأ المصطلح المعروف بدورة تطوير البرمجيات الآمنة (Secure SDLC) في قاموس تقنية المعلومات.

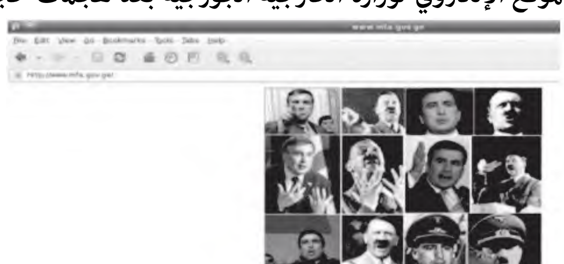
الشكل (١-٥): أحد محلات تي جي ماكس (T.J.Maxx)



٢٠٠٨- هجمات الامتناع عن الخدمة في جورجيا: تزامناً مع الحرب العسكرية بين روسيا وجورجيا في عـام ٢٠٠٨ كانت جورجيا ضحية لهجمات هائلـة ومنتشرة لحجب الخدمات الإلكترونية. وشوهت هذه الهجمات العديد من المواقع الإلكترونية التابعة لوسائل الإعلام والأجهـزة الحكومية بهدف الحد من قدرة هذه المواقع عـلى تواصل المواطنين فيما بينهم بخصوص وجهات النظر المختلفة حول الحرب (الشكل ١-٦). وأدت ملابسات هذا الحادث إلى الاعتقاد بأن روسيا كانت وراء تلك الهجمات الإلكترونية كجزء من إستراتيجية الحرب[١٢] . وإذا كان الأمر كذلك فإن هذه المرة الأولى التي تُسـتخدم فيها الهجمات الإلكترونية أداة في الحروب.

(١٢) مقطع (سايبر) يأتي في مقدمة الكلمات ذات العلاقة بأجهزة الحاسب الآلي والشبكات.

الشكل (١-٦): الموقع الإلكتروني لوزارة الخارجية الجورجية بعد هجمات حجب الخدمة



يونيو من عام ٢٠٠٩- تأسيس الأسطول الأمريكي لمكافحة الجرائم الإلكترونية: في شهر إبريل من عام ٢٠٠٩ ذكرت صحيفة وول ستريت جورنال أن مجموعة من المتسللين تمكنوا من اختراق الشبكة الحاسوبية لمقاولي وزارة الدفاع المسؤولين عن تطوير مشروع الطائرات المقاتلة المشتركة (Joint Strike Fighters)، ويُسمى أيضاً (F-٣٥ Lightning II)[١٣]، والذي تبلغ تكلفته ٣٠٠ مليار دولار وهو الأعلى تكلفة من بين برامج وزارة الدفاع كافة. وقد تم استخدام ٧,٥ ملايين سطر من الشفرة الحاسوبية في هذا المشروع. وقد تمكن المتسللون من سرقة بيانات ضخمة تتعلق بتصميم الطائرات والإلكترونيات. وكان يُعتقد أن هذه العملية ستساعد الأعداء على تطوير دفاعاتهم للتغلب على الطائرات المقاتلة المشتركة. أما المقاولون المشاركون في هذا المشروع فهم: (Lockheed Martin, Northrop Grumman, BAE Systems). وفي شهر إبريل أيضاً ذكرت صحيفة وول ستريت جورنال أن شبكة الكهرباء في الولايات المتحدة قد تم اختراقها من قبل جواسيس من الصين وروسيا ودول أخرى. وتمكن الجواسيس من إدراج برمجيات حاسوبية يمكن استخدامها عن بعد لإحداث أضرار في شبكة الكهرباء[١٤].

وبعد ذلك بوقت قصير، وبالتحديد في الثالث والعشرين من يونيو من عام ٢٠٠٩، تم تأسيس الأسطول الأمريكي لمكافحة الجرائم الإلكترونية لحماية الشبكات الحاسوبية التابعة لوزارة الدفاع من هجمات الأعداء، وذلك للقيام بكل ما من شأنه حماية الشبكات الحاسوبية. وفي وقت تأسيس هذا الأسطول الجديد كانت هناك مخاوف من فرض قيود لا داعي لها على الاستخدام المدني للإنترنت بحجة الدفاع عن البلاد.

(13) Gorman, S., Cole, A. and Draezen, Y. "Computer spies breach fighter-jet project," Wall Street Journal, April 21, 2009.

(14) Gorman, S. "Electricity grid in US penetrated by spies," Wall Street Journal, April 8, 2009.

٢٠١٠- عمليــة أورورا وجوجــل - الصين: في الثاني عشر من يناير من عام ٢٠١٠ أعلن مدير شركة جوجل للشؤون القانونية في مدونته الإلكترونية أنه اكتشف محاولة لسرقة حقوق الشركة الفكريــة، وهذه المحاولة قادمة من الصين (الشــكل ١-٧). واســتهدفت هــذه المحاولة أيضاً الوصول إلى رسائل البريد الإلكترونية لبعض الناشطين الصينين في مجال حقوق الإنسان. صعدت الحكومة الأمريكية هذا الحادث مع الكونغرس لتعلن نيتها عن التحقيق في هذه الادعاءات، كما وصــف وزير الخارجية الأمريــكي الرقابة الصينية على الإنترنت بحائط برلين في العصر الحديث. وأوضحــت التحقيقــات المتتالية أن مصــدر الهجمات أتى من اثنتين من المؤسســات التعليمية في الصــين (Shanghai Jiaotong University) و(Lanxiang Vocational School). وتُعــد المؤسســة التعليمية الصينية الأولى موطناً لأفضل برامج علوم الحاســب الآلي في الصين، في حين تشــارك المؤسســة التعليمية الصينية الثانية في تدريب علماء الحاســب الآلي التابعين للجيش الصيني[١٥]. لكن الصين نفت التدخل الحكومي الرسمي في هذه الهجمات، وقالت إن مثل هذه الهجمات هي محاولات للطلاب لصقل مهاراتهم في الحاسب الآلي.

الشكل (١-٧): مكاتب شركة جوجل في الصين

١٧ إبريل، ٢٠١١- شبكة سوني بلاي ستيشن (Sony PlayStation Network): أعلنت شركة ســوني عــن حدوث هجــمات خارجية على كل من شــبكة بلاي ستيشــن وخدمات (Qriocity service). وحصــل المهاجمون على المعلومات الشــخصية لأكثر من ٧٠ مليون مشترك. ولم تستبعد الشركة احتمالية سرقة بيانات بطاقات الدفع الائتمانية. ونتيجة لذلك

---

(15) Markoff, J. and Barboza, D. "2 China schools said to be tied to online attacks," New York Times, February 18, 2010,http://www.nytimes.com/2010/02/19/technology/19china.html (accessed January 8, 2012).

قامت الشركة بفصل خدماتها عن الشبكة حتى يتم التأكد من أن البرمجيات الخبيثة تمت إزالتها بشكل كامل من الشبكة. وخلال ذلك الوقت كان الملايين من الأطفال من جميع أنحاء العالم يخططون لقضاء إجازتهم الصيفية للعب إلكترونياً على شبكة بلاي ستيشن، لكن وبسبب هذه الحادثة توجب عليهم البحث عن بدائل أخرى لقضاء وقتهم. وعلى الرغم من اعتبار هذا الهجوم غير ضار نسبياً على الشبكة، إلا أن الأثر كان ضخماً على الأسر في جميع أنحاء العالم حيث كانت كل عائلة لديها أطفال تتابع التطورات اليومية لهذا الحادث.

هذا التسلسل الزمني الوجيز يبرز كيف تطورت هجمات أمن المعلومات من مرحلة إثبات نجاح مفاهيم الهجمات الإلكترونية إلى مرحلة القيام بالهجمات بدوافع تجارية لسرقة معلومات بطاقات الدفع الائتمانية. وحتى وقت متأخر كان الاشتباه حتى في الحكومات بأنها تستخدم الجرائم الإلكترونية لتنفيذ برامجها. وفي أوروبا برزت مدينة رومانية نائية، تدعى رمينكو فيلتش، كنقطة محورية عالمية في غسيل الأموال الناتجة عن جرائم الإنترنت. وفي مكان بعيد من هذه المدينة يوجد وكلاء لبيع سيارات مرسيدس بنز والسيارات الفارهة الأخرى[١٦]. وبالإضافة إلى ذلك فإن الاستجابة الاجتماعية للجرائم الإلكترونية قد تطورت أيضاً. فنرى القضاة يحذرون المتطفلين على شبكات الإنترنت، والقوانين تمنح استثناءات محددة للقُصّر على الرغم من مشاركتهم المعروفة في الهجمات الإلكترونية (كعصابة ٤١٤)، والحكومات تؤسس أساطيل عسكرية للتعامل مع أمن الإنترنت.

تعريف أمن المعلومات:

ومما سبق تتضح خلفية اهتمام المنظمات بأمن المعلومات. وإذا كنت متتبعاً لمثل تلك القضايا فإنك ستلاحظ أن تلك الحوادث لها تأثيرات مختلفة في أمن المعلومات. ففي حادثة عصابة ٤١٤ كانت المشكلة الكبرى في فقدان الخصوصية. وفي حالة أنرون كان التأثير في دقة المعلومات. وفي حالة جورجيا كان التأثير في قدرة المواطنين للوصول إلى المعلومات المطلوبة. ومن ثم فإن مفهوم أمن المعلومات قد يختلف باختلاف الأشخاص.

(16)Bhattacharjee, Y. "How a remote town in Romania has become cybercrime central," Wired Magazine, January 31, 2011,http://www.wired.com/magazine/2011/01/ff_hackerville_romania/all/1 (accessed January 8, 2012).

ويُعرّف أمن المعلومات بأنه حماية كل من المعلومات ونظم المعلومات من الأعمال غير المصرح بها كالوصول أو الاستخدام أو الإفشاء أو الإخلال أو التعديل أو التدمير وذلك لضمان التكامل، والخصوصية، والجاهزية.

وعلى الرغم من أن التعريف أعلاه يستند إلى مدونة قانون الولايات المتحدة الأمريكية (القسم ٣٥٤٢، الفصل ٣٥، عنوان ٤٤)[١٧]، إلا أنه يتسق بشكل ملحوظ مع تعريفات قطاع الأعمال. على سبيل المثال، تشير طلبات الملاحظات (RFC)[١٨،١٩] المنشورة من فريق عمل هندسة الإنترنت (Internet Engineering Task Force) والمتعلقة بأمن المعلومات، إلى أن الأهداف الأساسية للأمن هي: التكامل، والخصوصية، والجاهزية.

المختصر الثلاثي المكون من الحروف التالية C.I.A:

يذكر المتخصصون في القانون الأبعاد الثلاثة لأمن المعلومات بهذا التسلسل: التكامل (Integrity)، والخصوصية (Confidentiality)، والجاهزية (Availability). لكن هذه الأبعاد الثلاثة يمكن تذكرها بشكل أفضل إذا وضعناها في تسلسل مختلف قليلاً وهو المختصر الثلاثي المكون من C.I.A حيث الحرف (C) يرمز للخصوصية (Confidentiality)، والحرف (I) يرمز للتكامل (Integrity)، والحرف (A) يرمز للجاهزية (Availability). وللحفاظ على التناسق في هذا المختصر الثلاثي المشهور، سنناقش أبعاد أمن المعلومات في هذا التسلسل: الخصوصية، والتكامل، والجاهزية.

الخصوصية:

وفقاً للمادة ٣٥٤٢ من قانون الولايات المتحدة فإن الخصوصية تعني الحفاظ على القيود المُرخّصَة للإذن بالدخول إلى الأنظمة والإفصاح عن المعلومات، متضمناً ذلك وسائل حماية الخصوصية الشخصية والمعلومات السرية.

(١٧) توجد مدونة قانون الولايات المتحدة على شبكة الإنترنت من مصادر عديدة، لكن الناشرين في كثير من الأحيان يقومون بتغيير الرابط الإلكتروني في مواقعهم الإلكترونية. فمن الأفضل البحث عن المدونة بكتابة (٣٥٤٢ US code) في جوجل للعثور الموقع الإلكتروني. وفي الثامن من يناير من عام ٢٠١٢ كانت النتيجة الأعلى لكلية الحقوق في جامعة كورنيل على الرابط التالي: http://www.law.cornell.edu/uscode/usc_sec_٤٤_٠٠٠٠٣٥٤٢----٠٠٠-.html

(١٨) يُقصد بـ (RFC) طلب التعليقات (Requests for Comments) وهي الوثائق التي نشرها فريق عمل هندسة الإنترنت وهي المجموعة التي تحدد معايير الإنترنت بما في ذلك الـ (TCP/IP)

(19) Fraser, B. RFC 2196 site security handbook, September 1997, http://www.ietf.org/rfc/rfc2196.txt

ويؤكد القانون حق الأفراد في الخصوصية، وهذا الحق يشمل المعلومات التي قد يتسبب نشرها بإحداث أضرار أو إحراج للشخص. وتُعد الخصوصية إحدى مسؤوليات القائمين على المعلومات وذلـك لضمان خصوصية معلومات الأفراد التـي يملكونها. وجميع أمثلة سرقة بيانات بطاقات الدفع الائتمانية التي تمت مناقشتها في هذا الفصل تتعلق بفشل المنظمات في الحفاظ على سرية المعلومات التي في حوزتهم.

وإذا طلبت تعريفاً لأمن المعلومات من العامة فإن معظم الناس ستكون إجابتهم مقاربة للتعريف التالي: «أمن المعلومات يعني عدم فقدان بيانات بطاقات الدفع الائتمانية» حيث يربط معظم الناس أمن المعلومات بالخصوصية.

التكامل:

التكامل يعني الحماية من تعديل المعلومات أو تدميرها، ويشـمل ذلك التأكد من عدم إنكار المعلومات ومصداقية تلك المعلومات.

عنـد طلبـك تقريراً من أحد أنظمـة المعلومات كالدرجات الخاصة بـك في الجامعة أو كشـف حساب شهري من حسـابك المصرفي فأنت على يقين بأن معلومات التقرير موثوقة ويمكن الاعتماد عليها. على سـبيل المثال، عندما تسـتلم كشف رصيد حسابك البنكي فإنك لا تشـعر بضرورة التحقق من أرقام العمليات الحسـابية الخاصة بالرصيد الدائن والمدين وإيـرادات الفوائد. وبـدلاً من ذلك فإنك تثق بأن البنك قام بعمل الحسـابات الصحيحة. تخيل كيف أن الحياة ستكون معقدة في حال عدم الوثوق بدقة المعلومات التي تتلقاها من الأنظمة التقنية. التكامل هو بعد أمن المعلومات الذي يمنع حدوث ذلك.

في الأمثلة التي ناقشـناها أعلاه، فإن عدم قدرة الأنظمة التقنية من منع كبار المسؤولين في شركة أنرون، وشركة وورلدكوم من التلاعب بسجلات الشركة لخدمة مصالحهم الشخصية أمثلة على فشل التكامل.

الجاهزية:

الجاهزية تعني ضمان الوصول الموثوق للمعلومات واستخدامها في الوقت المناسب.

عند تسـجيلك الدخول لصفحة الإنترنت الخاصة بمقررك الدراسي فإنك تتوقع أن يكون المقـرر الدراسي موجوداً على صفحة الإنترنت وهذا في جوهـره يمثل الجاهزية. إن أهمية الجاهزيـة لأمن المعلومات واضحة ولا تحتاج إلى تفسـير. نظـام المعلومات غير المتاح هو نظـام معلومات غـير مفيد. وفي الأمثلة أعلاه، جاء رد شركة سـوني بلاي ستيشـن (Sony PlayStation Network) بوصفه أحد الأمثلة على فشـل الجاهزية. ولمعظم الفيروسـات الحاسوبية أيضاً الأثر نفسه المتمثل في حذف الملفات المهمة مما يؤدي إلى فقدان الجاهزية. حتى إذا كان بالإمكان في نهاية المطاف استعادة الملفات من أنظمة النسخ الاحتياطي أو من مصادر أخرى، فإن الوقت الضائع في اسـتعادة تلك الملفات لم يتم استغلاله بالشكل الأمثل ويمثل فقداناً للجاهزية.

حق الخصوصية:

مـن بين أبعاد أمن المعلومـات الثلاثة، ربما كان تعريف الخصوصيـة تعريفاً دقيقاً هو الأكثر صعوبة، وذلك لأن التوقعات الاجتماعية من الخصوصية متغيرة بشكل كبير. ما يعده شـخص ما خاصاً، كالصور على سـبيل المثال، لا يكون كذلك عند شخص آخر، وما كان يُعد خاصاً في السابق قد لا يُعد كذلك الآن. وبينما تحمي المنظمات خصوصية الموظفين بشكل كبير، قد لا يمانع هؤلاء الموظفون من مشاركة المعلومات نفسها وبطيب خاطر على شبكات التواصـل الاجتماعي والمواقـع الأخرى. وفي الواقع فإن حق الخصوصية يُعد حديثاً نسـبياً في القانـون الأمريكي. وجاءت أول إشـارة حديثة لحق الخصوصيـة في عام ١٨٩٠ في مقال في مجلـة هارفارد للويس برانديز (الـذي أصبح قاضي محكمة العدل العليا لاحقاً) وشريكه صموئيل وارن[٢٠].

الاختراعـات وطرق إدارة الأعمال الحديثة تلفـت الانتباه إلى الخطوة التالية التي يجب اتخاذها لحماية الشـخص وتأمينه وهو ما يُسـميه القاضي كولي «عدم التدخل في الشؤون الخاصـة». لقـد اعتدى المصـورون الفوريون والمؤسسـات الصحفية على قدسـية الحياة الداخليـة الخاصـة. وأصبحت العديد من الأجهـزة الآلية تهدد بتحقيـق التوقع بأن «ما يُهمس به في الخزانة سـوف يذاع على سـطح المنزل». ولسـنوات كان هنـاك اعتقاد بأن

(20) Brandeis, L.D. and Warren, S.S. "The right to privacy," Harvard Law Review, December 15, 1890, 4(5):http://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html (accessed 1/12/2012).

القانون يجب أن يتحمل مسؤولية علاج التداول غير المصرح به للصور الخاصة بالأشخاص؛... ونرى بأن الصحافة تتجاوز في كل اتجاه الحدود الواضحة لآداب وأخلاق المجتمع. ولم تعد الإشـاعات تصدر من الكسول والشرير بل أصبحت مهنة مرغوباً فيها من قطاعات الأعمال ويتم تداولها بكل جرأة... وأصبح الفرد معرضاً للضغوط النفسية والضيق من خلال انتهاك المؤسسـات الحديثة واختراعاتها لخصوصية الفرد وهذه الضغوط النفسـية أكبر بكثير مما يمكن أن تسببه الإصابات الجسدية.

وكان هـذا المقـال ناتجاً عـن موجة غضب من قبـل صموئيـل وارن رداً على التغطية الإعلاميـة لأحداث المجتمع الراقي في ذلك الوقت، متضمنـاً ذلك الأحداث التي جرت على عائلة وارن والتي كانت تتبع العادات الاجتماعية السائدة في ذلك الوقت مما سبب إحراجاً كبـيراً لعائلـة وارن[٢١]. وقد يجد القارئ تشـابهاً غريباً بين هذه الأفكار من القرن التاسـع عشر وبين مناقشـات الخصوصية في القرن الواحد والعشرين المتعلقة بالفيسـبوك وغيرها من مواقع التواصل الاجتماعي[٢٢]. وفي السنوات الأخيرة ومع زيادة مخاوف المنظمات على أمن المعلومات اقترح العديد من الخبراء توسـيع تعريف أمن المعلومات ليشـمل جوانب أخـرى مثل عدم إمكانية الإنكار (مثلاً إذا قامت شركة بخصم تكاليف خدمة تم طلبها عبر الهاتـف من بطاقتك الائتمانيـة وأنت تنفي طلب الخدمة، كيف يمكن إثبات أنك فعلاً من قـام بطلب الخدمة؟). لكن ولأهداف هذا المقرر الدراسي سـنركز على التعريف التقليدي لأمن المعلومات وأبعاده الثلاثة: التكامل، والخصوصية، والجاهزية.

دليل شخصي للحفاظ على أمن المعلومات:

إذا كنـت تدرس أمن المعلومـات ربما كان من الأفضل أن نبـدأ بحديث مقتضب لمدة دقيقتـين عن أمن المعلومات للإجابة عن السـؤال التالي: كيـف يمكنني الحفاظ على أمن المعلومـات بطريقة جيدة؟ وربما تتلقى هذا السـؤال من الأصدقاء وأفـراد العائلة الذين يشـعرون بالقلق حول أمـن المعلومات الخاصة بهم. وكل خبير سـيعطيك إجابة مختلفة استناداً إلى تجاربهم الخاصة. وهذه إجابتنا:

(21) Gordon Crovitz, L. "The right to privacy from Brandeis to Flickr," Wall Street Journal, 7/25/11.

(22) Facebook has a very well-written "Guide to Facebook security," at https://www.facebook.com/notes/facebook-security/ownyourspace-a-guide-to-facebook-security/10150261846610766..

إذا كنت ترغب في الحفاظ على أمن المعلومات الخاصة بك، يتوجب عليك القيام بما يلي للحصول على أفضل النتائج:

برامج مكافحة الفيروسات: تأكد أنك تستخدم برنامج لمكافحة الفيروسات وأن اشتراكك في هذا البرنامج حديث وغير منتهي الصلاحية. وكثير من الناس يمكنهم الحصول مجاناً على برامج مكافحة الفيروسات بوصفها جزءاً من اشتراكهم مع مزودي خدمات الإنترنت (ISP)، أو من أرباب العمل، أو من الجامعات والمدارس.

أتمتة تحديث البرامج: قم بضبط نظام التشــغيل والبرامج التطبيقية لتشغيل التحديث تلقائياً كلما كان ذلك ممكناً.

كلمات المرور: إذا كان ممكناً اســتخدم كلمة مــرور مختلفة لكل موقع يتطلب كلمة مرور. أما إذا كان ذلك صعباً فاســتخدم على أقل تقدير كلمتين من كلمات المرور: واحدة لمواقع المرح كمواقع النشرات الإخبارية والبريد الإلكتروني وما إلى ذلك، والأخرى للمنظمات الماليــة كالبنوك وشركات الوســاطة المالية. وفي أي مكان كنت ومع أي شــخص تحدثت لا تفصح عن كلمة المرور المالية مطلقاً[٢٣]. وكوســيلة ســهلة للمزيد من الأمن، بطِّن كلمات المــرور بالرموز، مثلاً (pass-word) كلمة ليســت صعبة جداً لتذكرها لكنها إلى حد ما أكثر أمناً من (password).

الملخص:

قدم هذا الفصل لمحة موجزة عن أمن المعلومات. وبدأ هذا الفصل بذكر الأسباب التي أدت إلى اعتقاد الشركات بضرورة الاســتثمار في أمن المعلومات. كما تم التعرض لأنشــطة المتخصصين في أمن المعلومات والتي تأخذ معظم وقتهم. وكان هناك مراجعة سريعة لأهم حــوادث أمن المعلومــات التي حدثت في الربع الأخير من هذا القــرن. ورأينا اعتماداً على

(٢٣) تأتي هذه التوصية من حقيقة أن العديد من الجرائم تحدث عندما تقوم المواقع الإلكترونية بحفظ كلمات المرور بدون تشفير. وإذا تم اختراق هذه المواقع فإن القرصان سيتمكن من الحصول على كلمة المرور الخاصة بك وبالتأكيد سيقوم باستخدامها في مواقع البنوك الإلكترونية ومواقع الوساطة المالية. ولمعلومات مفيدة أكثر عن هذا الموضوع يُنصح بقراءة مقال جيمس فالوز, "Hacked!," The Atlantic, November 2011,http://www.theatlantic.com/magazine/archive/2011/11/hacked/8673/ (accessed 01/12/13)

هذه الخـبرات أن قطاعات الأعمال قامت بتعريف أمن المعلومات متضمناً المختصر الثلاثي المكـون من C.I.A: الخصوصيـة (Confidentiality)، والتكامل (Integrity)، والجاهزية (Availability).

وفي بقية هذا الكتاب سـنركز على كيفية تطوير المهارات اللازمة لتطبيق أمن المعلومات حيث نبدأ بأساسـيات إدارة النظم والبرمجة لتمكين الطلاب مـن التفاعل مع التكنولوجيا خـلال الفصـل الدراسي. ونركـز على مهـارات إدارة النظم والبرمجة لأننـا نعتقد أن هذه المهـارات مـن عناصر المفاضلة الهامة عـلى الوظائف وخاصة للموظفـين المبتدئين. وبعد ذلك ننتقل إلى الموضوعات النظرية في القسـم الثاني من الكتاب. ولتطبيق أمن المعلومات نسـتعرض نموذجاً يتكون من الأصول، والثغرات الأمنية، والتهديدات، والضوابط. وسـوف نوضـح كيف يتم تحديد الأصـول والتهديدات، وكيف يتم التعامل مـع الحوادث. وأخيراً سندرس المجالات الإدارية والتنظيمية في القسم الثالث من هذا الكتاب.

نموذج حالة - ويكيليكس، كيبلقيت، والسيطرة الكاملة على مجموعة من الشبكات:

في شهر فبراير من عام ٢٠١٠ بدأ موقع ويكيليكس غير المعروف نسبياً بنشر مجموعة من المذكرات السرية من سجلات وزارة الخارجية الأمريكية. وفي صيف عام ٢٠١٠ وصل موقع ويكيليكـس إلى اتفـاق مع الصحف الرائدة في مختلف أنحاء العـالم، متضمناً ذلك صحيفة نيويـورك تايمز في الولايات المتحدة الأمريكية وصحيفة دير شـبيغل في ألمانيا، لنشر برقيات مختارة من السـجلات بصيغة منقحـة أي بعد إزالة المعلومات التعريفية من السـجلات. وأول هذه البرقيات تم نشرها في شـهر نوفمبر من عام ٢٠١٠. وبحلول شـهر سـبتمبر من عام ٢٠١١ تم اختراق أمن ملفات ويكيليكس بحيث أصبح أي شخص يستطيع رؤية جميع المذكرات بشـكلها الكامل على الإنترنت. وتم تصنيـف قرابة نصف المذكرات المسربة بأنها «غـير خاصـة»، و (٤٥٪) تم تصنفيها بأنهـا «خاصة»، والباقي تم تصنيفهـا بأنها «سرية» . ولم يتـم تصنيف أي من المذكرات بأنهـا «سرية للغاية». وحصلت هذه الحادثة على لقب كيبلغيت (Cablegate).

ويكيليكـس هي منظمة غـير ربحية بدأت في عام ٢٠٠٧. ويُعد جوليان أسـانج القوة الرئيسـية وراء ويكيليكـس. وهو مبرمج كمبيوتر مميز وقدير من أسـتراليا، ولديه حماس

قوي للإصلاح المُعتمِد على حرية الصحافة. وبناءً عليه فإن مهمة ويكيليكس هي مساعدة الأشـخاص الذين يرغبون بالتبليغ عن المخالفات والفسـاد وإيصالهـا إلى الصحيفين بدون معرفـة هوياتهـم، وذلك من خلال توفير صندوق اسـتلام إلكتروني آمـن ولا يطلب هوية المسـتخدم. كما يأتي موقع ويكيليكس بدافع من مبادئ حرية الكلام وحرية النشر لوسائل الإعلام. كما أن ويكيليكس فخورة بسـجلها في الدفاع عـن الصحفيين، وفخورة أيضاً بعدم تحديد هوية مصادرها ضد الهجمات القانونية والسياسية التي تهدف للحصول على هويات هذه المصادر.

وتُعـد المذكـرات التي تم تسريبها من قبل ويكيليكس نتيجـة جهد عقود من الزمن في جمع المعلومات عن طريق المكاتب الدبلوماسـية الأمريكية في جميع أنحاء العالم. وتعود أقـدم مذكرة إلى عـام ١٩٦٦، وكان تسريب المذكرات مصدراً لإحـراج كبير لوزارة الخارجية الأمريكية. ولخصت المذكرات المسربة تحليلات قام بها قادة العالم والدبلوماسيين الأمريكيين. وانعكاسـاً للمواقف الجيوسياسـية جاءت هذه التحليلات غالباً على خلاف المواقف العامة للقـادة. وتعتمد رغبة القادة في مشـاركة تحليلاتهم في المقـام الأول على الثقة الكاملة في قـدرة وزارة الخارجية الأمريكية على الحفاظ على سرية المعلومات وعلى هوياتهم. ولعدم وجود تسريب للمعلومات في الماضي تمتع الدبلوماسـيون الأمريكيون في جميع أنحاء العالم بدرجة عالية من المصداقية في السلك الدبلوماسي، وهذا سمح لهم بالوصول إلى المعلومات الحساسة والمتميزة.

وفي الواقع متى جرى تسريب المذكرات فإن الصحف الرائدة في العديد من الدول تقوم بنـشر مقتطفات من المذكرات التـي تتعلق ببلادهم لإرضاء فضول القـراء حول ما تعرفه الولايات المتحدة الأمريكية عن وطنهم.

المصدر - الجندي أول برادلي مانينغ:

بـرادلي مانينـغ هو جنـدي أول في الجيش الأمريـكي كان عمره ٢٣ عامـاً وقت حادثة كيبلغيت. تجند برادلي في الجيش الأمريكي في عام ٢٠٠٧ وتدرب ليصبح محلل استخبارات. وخلال هذا الوقت تمكن برادلي باستخدام علاقاته من التواصل مع أحد المبرمجين المتحمسين لخدمـة المجتمع وهو من جامعة برانديز بالقرب من بوسـطن. وفي عام ٢٠٠٨ كان برادلي

أحــد الجنود الذين تم نشرهم في العراق، وأعطته وظيفتــه هناك صلاحية الدخول لاثنتين من شــبكات المعلومات: الأولى (SIPRNet)، والثانية نظام الاتصالات الاستخباراتي العالمي المشترك (JWICS). ويمتلك أكثر من ثلاثة ملايين موظف حكومي أمريكي صلاحية الدخول لهاتين الشبكتين. وجاءت صلاحية الدخول الواسعة لهاتين الشبكتين نتيجة لهجمات الحادي عشر من ســبتمبر حيث كان يُعتقد أن العجز الموجود في تبادل المعلومات داخل الحكومة كان مسؤولاً - ولو جزئياً - عن فشل الحكومة الأمريكية في صد تلك الهجمات.

ومــن خلال تلك الشــبكتين حصل الجندي أول مانينغ عــلى المذكرات المُسربة. وما بين عامــي ٢٠٠٩ و٢٠١٠ قــرر تمريــر هذه المذكــرات السرية إلى ويكيليكس. وفي شــهر مايو مــن عــام ٢٠١٠ عرضت مجلة (Wired) بعــض المعلومات عن مجتمــع قراصنة الإنترنت وبالتحديــد عرضت معلومات عن شــخص يُدعى أدريان لامو وهو أحد قراصنة الحاســب السابقين. ويُعتقد أنه نتيجة لهذا المقال قام الجندي أول مانينغ بالاتصال بقرصان الحاسب لامــو والحديث معه بواســطة برنامج الرســائل الفورية (AOL). وأثناء الحديث كشــف مانينــغ أنه قام بتسريب المذكرات كما أشــار إلى دوافعه للقيــام بذلك. وقرر لامو أن يخبر الســلطات بذلك مما أدى إلى اعتقال الجندي أول مانينغ وإفشاء هوية مصدر ويكيليكس. ونــشرت مجلة (Wirde) نص الحديث الــذي دار بين الجندي أول مانينغ وأدريان لامو[٢٤] . ومــن العبــارات المميزة في هذا النص (PM ١٢:١٥:١١): إذا كان لديك ســيطرة كاملة على مجموعة من الشــبكات لفترة طويلة من الزمن...لنقل ثمانية إلى تسعة أشهر...ورأيت أشياء لا تصدق، أشــياء مروعة...أشــياء موجودة للجميع على النطاق العام...وليست موضوعة في بعض الحواســيب الخادمة (Servers) المخزّنة في غرفة مظلمة في واشنطن العاصمة...ماذا كنت ستفعل؟

واتُهم الجندي أول مانينغ في اليوم الثالث والعشرين من شهر فبراير من عام ٢٠١٢ أمام محكمة عســكرية بارتكاب جرائم من بينها مســاعدة العدو. وعلى الرغم من أن مساعدة العدو جريمة كبرى تصل عقوبتها إلى الإعدام إلا أن النائب العام لم يســع إلى عقوبة الإعدام في هذه الحالة.

(24) http://www.wired.com/threatlevel/201107//manning-lamo-logs/

المراجع:

http://en.wikipedia.org/wiki/United_States_diplomatic_cables_leak

http://en.wikipedia.org/wiki/Bradley_Manning

http://www.bbc.co.uk/news/world١١٠٤٧٨١١-

http://www.wired.com/threatlevel/٠٧/٢٠١١/manning-lamo-logs/

http://www.cablegatesearch.net/

أسئلة مراجعة للفصل:

١. ما هي بعض نقاط القوة في أمن المعلومات كخيار وظيفي؟

٢. ما هي بعض الطرق التي يمكن من خلالها استخدام المعلومات المسروقة لتحقيق الأرباح؟

٣. ما هي بعض الطرق الأكثر شيوعاً والتي من خلالها يؤدي إهمال المستخدمين النهائيين إلى إمكانية فقدان المعلومات الحساسة؟

٤. ما هي بعض المسؤوليات المهنية المشتركة بين خبراء أمن المعلومات؟

٥. قدم وصفاً مختصراً لأنشطة خبراء أمن المعلومات والتي يقضون فيها معظم وقتهم.

٦. اشرح بشكل موجز أهم المهارات التي من المُتوقع أن تكون لدى خبراء أمن المعلومات لتحقيق النجاح في عملهم.

٧. كيف أثّر تطور تقنية الشبكات الحاسوبية (TCP/IP) غير المُكلِفة في أمن المعلومات؟

٨. اشرح بشكل مختصر أنشطة عصابة ٤١٤.

٩. اشرح بشكل مختصر تأثير عصابة ٤١٤ على أمن المعلومات.

١٠. صِف بشكل مختصر دودة موريس الخبيثة. ما العوامل التي تجعل منها نقطة بارزة في تطور أمن المعلومات؟

١١.ما تأثير نظام التشغيل (ويندوز ٩٨/٩٥) في أمن المعلومات؟

١٢.كيف أثر قانون إمكانية نقل التأمين الصحي والمساءلة (HIPPA) في وظائف أمن المعلومات؟

١٣.ما الأحكام الواردة في قانون ساربينز أوكسلي (Sarbanes-Oxley Act) والتي تتعلق بأمن المعلومات؟

١٤.ما العوامل المباشرة التي أدت إلى تأسيس الأسطول الأمريكي لمكافحة الجرائم الإلكترونية؟

١٥.قدم شرحاً مختصراً للأسطول الأمريكي لمكافحة الجرائم الإلكترونية والأنشطة التي يقوم بها.

١٦.ما عملية أورورا وجوجل التي تمت من الصين؟

١٧.اشرح بشكل موجز انقطاع الخدمة الذي أثر في شبكة سوني بلاي ستيشن في عام ٢٠١١.

١٨.ما أمن المعلومات؟

١٩.ما الخصوصية؟

٢٠.ما التكامل؟

٢١.ما الجاهزية؟

٢٢.أعط مثالاً على انتهاك الخصوصية.

٢٣.أعط مثالاً على انتهاك التكامل.

٢٤.أعط مثالاً على انتهاك الجاهزية.

٢٥.في رأيك ما أهم عنصر من عناصر أمن المعلومات الثلاثة؟ ولماذا؟

أسئلة على نموذج الحالة:

١. من أبعاد أمن المعلومات الثلاثة، أيها تأثر بحادثة كيبلغيت؟

٢. في اعتقــادك ما الذي دفع الجندي أول برادلي مانينغ لتسريب المذكرات لويكيليكس ومن ثم مناقشة تصرفه هذا مع أدريان لامو وهو يدرك جيداً مخاطر تصرفه هذا؟

٣. اســتناداً إلى المعلومات المعلنة والمتاحة، ما التدابير التي اتخذتها الحكومة الأمريكية لتأمين المذكرات؟

٤. وإلى أي مدى هذه التدابير فعالة؟

٥. لو كنت مسؤولاً عن أمن المعلومات المتعلق بهذه المذكرات، ما الذي ستقوم به لمنع وقوع الحوادث المشابهة لحادثة كيبلغيت؟

٦. وفي اعتقادك لماذا لم يقم الخبراء المســؤولون عن أمن المعلومات المتعلق بالمذكرات باتخاذ الإجراءات التي اقترحتها أعلاه؟

نشاط التدريب العملي - مراقب البرمجيات، إخفاء المعلومات:

في نهاية كل فصل تم تصميم أنشطة للتدريب العملي بهدف مساعدتك لمعرفة الأدوات المستخدمة من قبل خبراء أمن المعلومات. كما تساعدك هذه الأنشطة العملية على تطبيق المادة النظرية التي تمت مناقشتها في سياق أنظمة حقيقية.

برنامج سيكونيا لمراقبة البرمجيات (Secunia Online Software Inspector):

في أول نشــاط للتدريب العملي ستقوم باستخدام برنامج مجاني لتحديد أهم المشكلات الأمنية في أجهزة الحاسب الآلي التي تستخدم للعمل اليومي، وهذه العملية تسمى التدقيق. وأدوات تدقيــق أجهزة الحاســب الآلي متوفرة لدى شركات البرمجيــات ومزودي خدمات الإنترنت. وفي حين نســتخدم في هذا التمرين أداة التدقيق المقدمة من شركة (Secunia)، لك كامل الحرية في استخدام الأدوات المماثلة من الشركة المفضلة لديك.

وبرنامــج (Secunia Online Software Inspector) متوفــر في موقــع الشركــة[٢٥]، ويوضــح الشــكل (١-٨) الموقع الإلكتروني لهذا البرنامج. اســتخدام هــذا البرنامج واضح ومبــاشر. بالضغط عــلى زر (Start Scanner) في الصفحة يبــدأ بالفحص مع الخيارات الافتراضية، وتســتغرق عملية الفحص بضع دقائق. وعند الانتهاء يظهر التقرير في الجزء السفلي من الصفحة. ويوضح الشكل (١-٩) عينة من هذا التقرير.

الشكل (١-٨): مراقب البرمجيات الفوري



ويبين التقرير أن جهاز الحاســب الآلي المفحــوص يحتوي على العديد من التطبيقات البرمجية التي تحتاج إلى تحديث لآخر إصداراتها. وقد رأينا في هذا الفصل أن الإصدارات القديمــة للبرمجيــات، والتــي تعرف عــادة بالثغرات الأمنيــة، يمكن اســتغلالها من قبل الفيروســات الخبيثــة وقراصنة الإنترنــت. ومن الجيد أن نقوم بتشــغيل أداة من أدوات تدقيق الحاســب الآلي - كالأداة المســتخدمة في هذا التطبيق - ومن ثم تحديث أو حذف التطبيقات القديمة.

---

(٢٥) الروابط الإلكترونية متغيرة بشكل كبير. لكن في الثاني من ديسمبر من عام ٢٠١٢ كان الرابط (http://secunia.com/vulnerability_scanning/online/). وبالطبع فإن الطريقة الأفضل والأكثر موثوقية هي استخدام محرك البحث جوجل للعثور على (Secunia Online Software Inspector.)

Source: http://lifehacker.com/٢٣٠٩١٥/geek-to-live--hide-data-in-files-with-easy-steganography-tools

الشكل (١-٩): تقرير تدقيق جهاز الحاسب الآلي



أسئلة عن تدقيق أجهزة الحاسب الآلي:

شـغّل أداة مـن أدوات تدقيق أجهزة الحاسـب الآلي مثـل برنامـج (Secunia Online Software Inspector)، ثم قم بأخذ صورة من الشاشة لتقرير التدقيق المشابه للشكل (١-٩).

ما هي بعض الإجراءات التي تفكر باتخاذها بعد الاطلاع على نتائج تقرير تدقيق جهاز الحاسب الآلي الخاص بك؟

إخفاء المعلومات (Steganography)(٢٦):

هـذا التمرين يمنحـك الفرصة لإلقاء نظرة على "الجانب المظلـم" من أمن المعلومات. وستؤدي في هذا التمرين دور شخص ثوري يحاول إرسال رسالة سرية إلى أصدقائه. وتحاول في رسـالتك تحديد موعد ومكان للقاء مجموعة من الأصدقاء. وتعتقد أنه تم الاطلاع على جميع رسائلك الإلكترونية.

وهنـاك العديـد من الطرق للقيام بذلك لكن في هذا التمرين سنسـتخدم طريقة سـهلة وممتعة. سـوف تقوم بإخفاء النص مع المعلومات ذات العلاقة داخل صورة (شـعار الجامعة على سبيل المثال) ومن ثم إرسالها إلى أصدقائك. وإذا كان أصدقاؤك يعلمون أين يبحثون فإن

(26) Source: http://lifehacker.com/230915/geek-to-live--hide-data-in-files-with-easy-steganography-tools

بإمكانهم بسهولة الحصول على المعلومات. والهدف من هذا التمرين هو توضيح مدى سهولة إنشاء تحديات لأمن المعلومات ومن ثم مدى صعوبة القضاء على مشكلات أمن المعلومات.

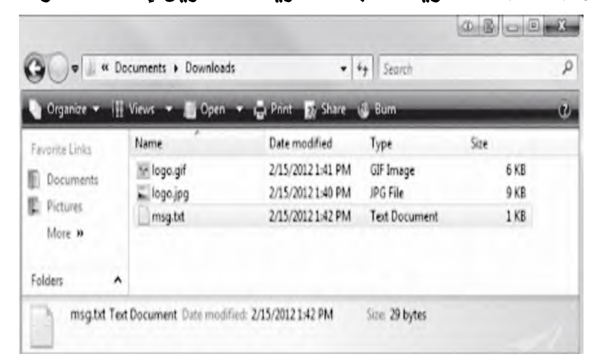
وللقيام بهذا التمرين ستحتاج إلى ما يلي:

ملــف صورة: في حين أن أي ملف صورة ســيؤدي الغرض، يفضــل أن يكون ملف الصورة صغيراً من نوع (jpg) أو (gif). وعادة صورة شــعار جامعتك ســيؤدي الغرض. احفظ الملف على جهاز الكمبيوتر الخاص بك. وفي هذا التمرين نفترض أن يتم حفظ جميع الملفات في مجلد التنزيلات لأنه موقع ملائم سواء على أجهزة الويندوز أو أجهزة الماك. ولهذا المثال سيكون اسم ملف الصورة logo.gif (إذا كان نوع الصورة gif) أو logo.jpg (إذا كان نوع الصورة jpg).

ملف نصي يحتوي على تاريخ ومكان ووقت الاجتماع: احفظ الملف في المجلد نفســه الذي فيه ملف الصورة أعلاه (وأســهل طريقة لإنشاء هذا الملف عن طريق برنامج المفكرة Notepad ومــن ثــم كتابة النص وحفظ الملف في مجلد التنزيلات). ولهذا المثال ســيكون اسم الملف msg.txt.

عند انتهائك مما سبق فإن مجلد التنزيلات سيبدو كما في الشكل (١-١٠).

الشكل (١-١٠): محتويات مجلد التنزيلات لتمرين إخفاء المعلومات



نحن الآن على استعداد لإخفاء الملف النصي داخل ملف الصورة. ولتحقيق ذلك تحتاج إلى فتح موجه الأوامر (Command prompt) والذي يمكن الوصول إليه في أجهزة الويندوز من خلال:

قائمــة جميع البرامــج (All programs) ← البرامج الملحقة (Accessories) ← موجه الأوامر (Command Prompt) أما في أجهزة الماك فيمكن الوصول إليه من خلال:

تطبيقات (Applications) ← البرامج المساعدة (Utilities) ← الوحدة الطرفية (Terminal)

وللوصول إلى مجلد التنزيلات اكتب الأمر التالي في صفحة موجه الأوامر:

```
Cd Documents\Downloads
```

في أجهزة الويندوز الأمر التالي سيضيف الملف الثاني في نهاية الملف الأول ويحفظ الناتج في الملف الثالث:

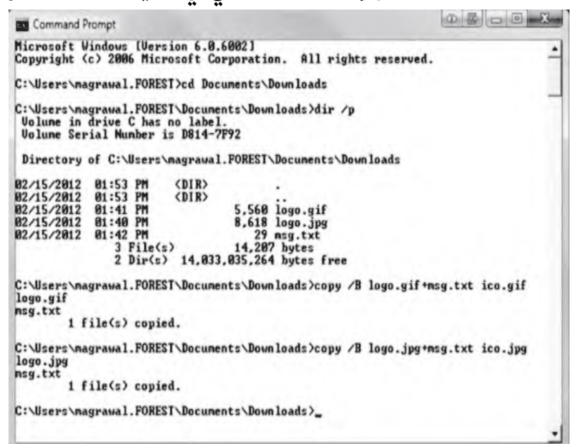
```
Cd Copy /B file1+file2 file3
```

ولاستخدام هذا الأمر بهدف إخفاء الملف النصي في ملف الصورة نستخدم الأوامر التالية:

```
Cd Copy /B file1+file2 file3
Copy /B logo.jpg+msg.txt ico.jpg (for the jpg image)
Copy /B logo.gif+msg.txt ico.gif (for the gif image)
```

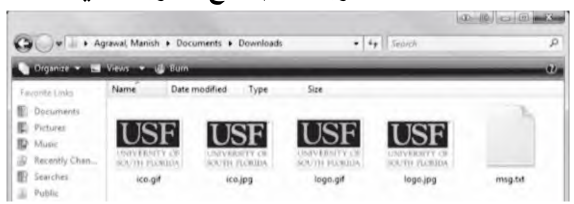
وتسلسل هذه الأوامر موضح في الشكل (١-١١).

الشكل (١-١١): أوامر إخفاء ملف نصي في نهاية ملفات الصور



بعد تشــغيل هذه الأوامر ســتظهر محتويات مجلد التنزيلات كما في الشــكل (١-١٢) (وبالإمكان معاينة الصور عن طريق عرض ← أيقونات كبيرة).

الشكل (١-١٢): الصور المعالجة مع الصور الأصلية

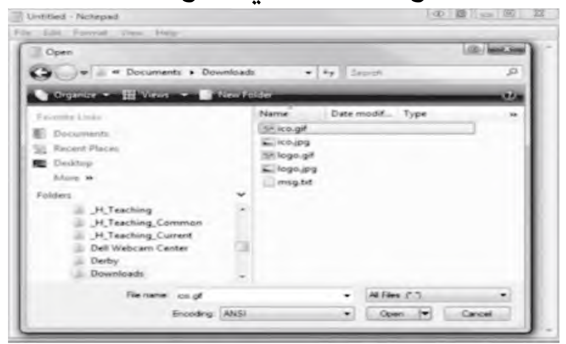


وقــد تلاحــظ أن الصور المعالجــة (ico.gif and ico.jpg) لا يمكــن تمييزها عن الصور الأصلية (logo.gif and logo.jpg). والشــخص الذي ليس على علم بأنشــطتك لن يلاحظ أي نقــص في الصور المعالجة. وبإمكانك التحقق من أن هذه الصور يمكن فتحها في برنامج المتصفح وبقية التطبيقات الأخرى. كما يمكنك التحقق من أنه يمكن استخدام هذه الملفات بشكل مطابق لاستخدام ملفات الصور الأخرى.

لكن كيف يتمكن أصدقاؤك من استرداد المعلومات المخفية في الصور؟

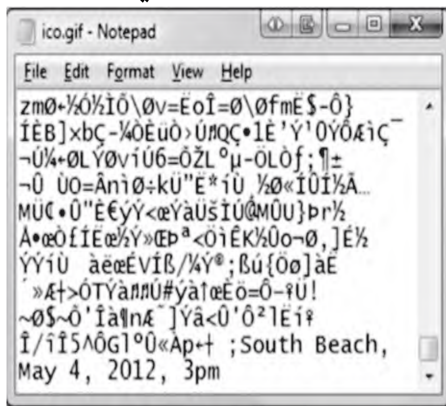
ويتضح أنه من السهل عليهم القيام بذلك من خلال استخدام التطبيق المناسب وهو في هذه الحالة برنامج المفكرة (Notepad). قُم بتشــغيل برنامج المفكرة Notepad ثم اختر ملف ← فتح، ثم انتقل إلى مجلد التنزيلات. قُم بتغيير نوع الملف إلى كافة الملفات (*.*) كما في الشكل (١-١٣) واختر إما ملف (ico.gif) وإما ملف (ico.jpg).

الشكل (١-١٣): فتح ملفات الصور في برنامج المفكرة Notepad



تجاهل النص غير المقروء وانتقل إلى نهاية الملف وســوف ترى شيئاً مماثلاً لما في الشكل (١-١٤).

الشكل (١-١٤): الرسالة السرية المخفية في نهاية ملف الصورة



وتــرى أنه مــن الممكن خلق تحديات مثــيرة لأمن المعلومات باســتخدام أدوات تقنية بســيطة ومتوفرة للجميع. وقد تُدرك الآن أن هذه الإمكانات قد تسبب الذعر لخبراء أمن المعلومــات. ما قمت به في هذا التمرين يُدعى إخفاء المعلومات (Steganography) وهو إخفاء المعلومات بطريقة لا يشك أحد في وجودها.

أسئلة على تمرين إخفاء المعلومات:

أنشئ صورة فيها معلومات مخفية باتباع إرشادات هذا القسم.

قدم نسخة مطبوعة لكل مما يلي: الصورة الأصلية والصورة المعالجة ولقطة من الشاشة للنص المضمن في الصورة كما في الشكل (١-١٤).

تمريــن التفكير النقدي: تحديد الأبعاد الثلاثة لأمن المعلومات المتأثرة بعينة من حوادث الاختراق الواقعية:

قَدّم هذا الفصل بعضاً من حوادث أمن المعلومات الأكثر إضراراً والأكثر شهرة. ولتسهيل الرجوع إلى هذه الحوادث تم تلخيصها في الجدول (١-١).

الجدول (١-١): حوادث أمن المعلومات الرئيسية وأثرها

الحوادث	بعد أمن المعلومات المتأثر	التدابير الوقائية الممكنة
عصابة ٤١٤		
دودة موريس الخبيثة		
فيروس ILOVEYOU		
الهجمات الإلكترونية على تي جي ماكس		
المواقع الإلكترونية الحكومية في جورجيا		
مشروع الطائرات المقاتلة المشتركة		
جوجل - الصين		
شبكة سوني بلاي ستيشن		

ولــكل حادث من الحوادث المدرجة في الجدول حــدد بعد أمن المعلومات الأكثر تضرراً من بين أبعاد أمن المعلومات الثلاثة (الخصوصية، التكامل، الجاهزية). وعلى الرغم من أننا لم نناقش في هذا الفصل التدابير التي تأخذها المنظمات لحماية نفسها ضد هذه الأنواع من الحوادث، قُم بمحاولة أولية لتحديد بعض التدابير الوقائية التي يمكن للمنظمات القيام بها للتأكد من أن هذه الحوادث لن تحدث لها.

تصميم حالة:

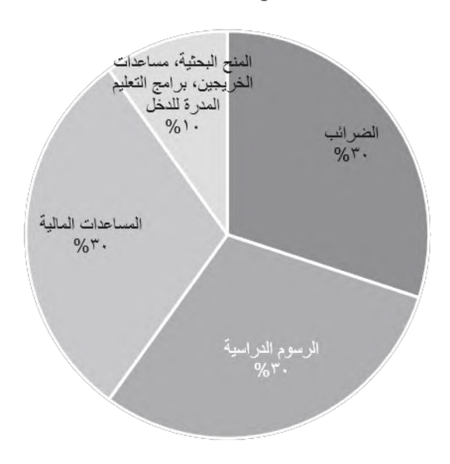
ولإعطاء الطلاب شرحاً مفصلاً عن عملية تطوير هيكل أمن المعلومات للمنظمة تم تصميم حالة مترابطة بجميع موضوعات فصول الكتاب. وفي كل فصل ســنقوم باستخدام المفاهيم التي جرى التعرض لها في الفصل لبناء هيكل أمن المعلومات للمنظمة. وللمساعدة في هذا التمرين تم ترتيب فصول الكتاب بتسلســل مقارب لتسلسل التعامل العملي للموضوعات ذات العلاقة بأمن المعلومات. ولذلك فإن أنشطتك في الفصول المتقدمة ستساعدك على بناء الحل في الفصول المتأخرة. والمنظمة التي سنتعرض لها في هذه الحالة هي جامعة حكومية تقليدية. وتشترك الجامعات الحديثة مثل جامعة ولاية الشمس المشرقة (Sunshine State University) في معظم خصائص المنظمات المتوسطة والكبيرة حيث تخدم هذه الجامعات ما يزيد على ٢٠,٠٠٠ مســتخدم ويعمل فيها آلاف الموظفين ولديها ميزانيات تتجاوز مليار

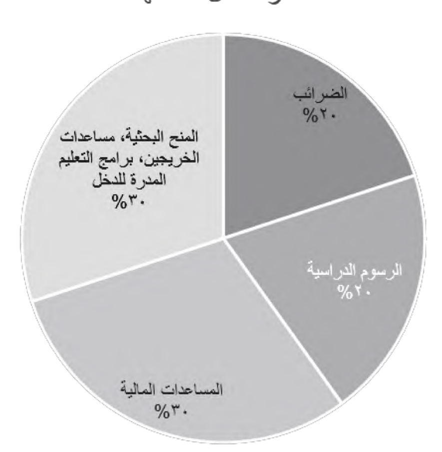
دولار، ويجــب أن تَمْتَثِـل هذه الجامعات لتنظيمات وقوانين متعــددة. ولتلبية احتياجات جميع هؤلاء الفئات يوجد في الجامعات جميع عمليات منظمات قطاع الأعمال ونظم تقنية المعلومــات التي توجــد في أي شركة تقليدية كالموارد البشرية، والرواتب، والمالية، والســفر بالإضافــة إلى الخدمات التقليدية كالبريد الإلكتروني والتقويــم. ويعمل العديد من المراكز البحثية بمثابة الأوصياء على البيانات الشــخصية الحساســة المرتبطة بالمشاريع البحثية مما يــؤدي إلى خلق احتياج لأمن المعلومات بشــكل مماثل لاحتياج أمــن المعلومات في معظم الــشركات الكبــيرة. وفي الواقع فإنه من غير المســتغرب أن نجد انتشــاراً لتقنية المعلومات الرائدة في الجامعات الحكومية. ومن وجهة نظر الطلاب وأعضاء هيئة التدريب فإن الميزة العظمى لاستخدام الجامعة في سياق تصميم الحالة المترابطة أنها مألوفة جداً لدى الجميع. وإذا لــزم الأمر فإنه يمكن لأعضاء هيئة التدريس أن يغيروا في ســياق الحالة ليتناســب مع الاحتياجــات الخاصة بمنظماتهم. وفي معظم الحالات فإن الطلاب قد واجهوا بعض القضايا التي تمت مناقشتها في الحالة مما يسهل عملية التعلم بشكل كبير.

المنظمة:

جامعة ولاية الشــمس المشرقة (Sunshine State University) هي جامعة حكومية. ومثل العديد من الجامعات الحكومية يأتي (٣٠٪) من تمويل الجامعة من الضرائب المستحقة للدولة، و (٣٠٪) تأتي من الرســوم الدراســية للطلاب، و (٣٠٪) تأتي من المســاعدات المالية للطلاب (الشكل ١-١٥). والـ (١٠٪) المتبقية تأتي من مجموعة متنوعة من المصادر بما فيها المنــح البحثية، ومســاهمات الخريجين، وبرامج التعليم المدرة للدخــل كالتعليم التنفيذي. وتحــاول الجامعــة المضي قدماً نحــو المزيد من التميز عن طريق الحــد من اعتمادها على ضرائب الدولة والرســوم الدراســية لنحو (٢٠٪) لكل منهما. وسيتم تعويض الفرق بزيادة إيــرادات المصــادر الأخرى من (١٠٪) إلى نســبة (٣٠٪) من إجــمالي الميزانية. ويصل عدد الطلاب الملتحقين بجامعة ولاية الشــمس المشرقية إلى ٢٠,٠٠٠ طالب. ولتقديم الخدمات الأكاديميــة لهــؤلاء الطلاب يعمل في الجامعة ٧٠٠ عضو هيئة تدريس (ومن ثم فإن نســبة الطــلاب إلى أعضاء هيئة التدريــس تصل إلى ٢٩). وهناك أيضــاً قرابة ١٥٠٠ من موظفي الدعم الإداري يؤدون وظائف مثل الإرشــاد الأكاديمي، والمنح الدراسية، وتقنية المعلومات، والمالية، والمرتبات، ومديري المكاتب، وغيرها.

الشكل (١-١٥): مصادر الدخل في جامعة ولاية الشمس المشرقة





ولتحسين التجربة التعليمية للطلاب بدأت جامعة ولاية الشمس المشرقة بزيادة تركيزها على الفرص البحثية لطلاب الدراسات العليا وطلاب الدراسات الجامعية. وفي الوقت الحالي يقود هذا التوجه كلية الهندسة وكلية الطب، فلدى أعضاء هيئة التدريس المعينين مؤخراً في هاتين الكليتين سجلات قوية لجذب تمويل البحوث من مصادر مثل مؤسسة العلوم الوطنية (National Science Foundation) والمعاهد الصحية الوطنية (National Institutes

of Health). وبينما تخلق هذه المشــاريع فرصاً كبيرة للطلاب لكســب منحة دراسية أثناء العمل على المشــاريع البحثية، فإنه قد تم إبلاغ مديري الجامعات من قبل زملائهم أن على الجامعة ترقية أنظمتها للتعامل مع البيانات التي تم إنشاؤها بواسطة هذه المشاريع حيث تم تحويل العديد من الجامعات إلى المحاكم القضائية بسبب انتهاك خصوصية الموضوعات البحثية وخصوصية الطلاب(٢٧).

الهيكل التنظيمي:

يوضح الشــكل (١-١٦) ملخصاً للهيكل التنظيمي للجامعة. والمناقشــة في هذا الكتاب ســوف تكون مقصورة على وحدات الجامعة الموضحة في الهيكل التنظيمي. مدير الجامعة هو المســؤول عن جميع الشــؤون الأكاديمية في الحرم الجامعي. ومدير العمليات مسؤول عن جميع الأنشــطة المالية والعملية في الحرم الجامعي. أما المستشار العام فيدير الشؤون القانونية ومسؤول عن مدى الامتثال للوائح والأنظمة.

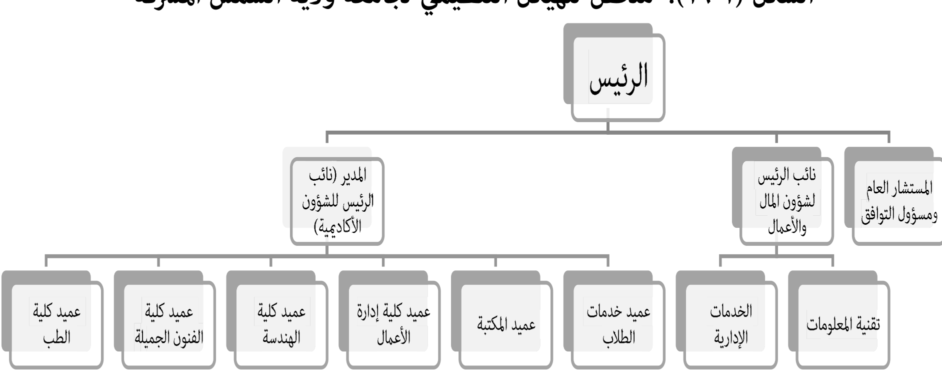
ويــؤدي طلاب كلية الطب برنامج الأطباء المقيمين في مستشــفى محلي وســط المدينة. ويعمل في المستشــفى نفســه، الذي يُعد جزءاً من شركة كبيرة متعددة الأنشطة، موظفون متخصصــون في دعــم تقنية المعلومات. وقد بدأ مشروع بحثــي كبير من قبل أعضاء هيئة التدريــس بالكلية يتضمن ٤٠٠٠ طفل حديث الولادة لدراســة التأثيرات الطبية للتفاعلات بين العوامل البيئية والتركيبات الجينية. وستقوم الدراسة بمتابعة هؤلاء الأطفال حتى تصل أعمارهم إلى ١٥ عاماً. وتحتفظ الكلية بالخدمات التكنولوجية والتي تتألف أساساً من توفير خدمات البريد الإلكتروني وحفظ المستندات المشتركة.

وتُعرف كلية الفنون الجميلة باســم مدرسة الفن والتي خرّجت العديد من فناني الرسم المشهورين. وعلى الرغم من أن الجامعة ليست موطناً للاستوديوهات السينمائية الرئيسية إلا أن مجموعة من الخريجين حديثاً قد استفادوا من القدرات التصويرية للكاميرات الرقمية ذات العدســة الأحادية العاكســة (DSLR cameras) لتحقيــق النجاح كمخرجين في دائرة الأفلام السينمائية المستقلة (إيندي)(٢٨).

(27) See http://blog.alertsec.com/2012/01/univ-of-hawaii-settles-data-breach-lawsuit/ for an example

(٢٨) تشير (إيندي) إلى دائرة الأفلام السينمائية المستقلة. وعادة ما يتم انتاج أفلام إيندي وتسويقها بميزانية صغيرة وبدون مساعدة من الاستوديوهات السينمائية الكبرى. وتمكن العديد من المخرجين السينمائيين المهمين من جذب الاهتمام أولاً في الأفلام السينمائية المستقلة.

الشكل (١-١٦): ملخص للهيكل التنظيمي لجامعة ولاية الشمس المشرقة



وبدأت كلية الهندسة في جذب انتباه المؤسسات التمويلية حيث بدأت تجذب بعضاً من التمويل الأولي من وزارة الدفاع الأمريكية لتطوير أجهزة الاستشعار والتطبيقات المرتبطة بها الخاصة بانتشار الجنود في ساحة المعركة.

وبالإضافة إلى الأنشطة التعليمية والبحثية التقليدية قامت كلية إدارة الأعمال بدعم الشركات المحلية ذات الأقلية في المجتمع من خلال توفير حاضنة للأعمال التجارية والتي تستطيع من خلالها (الشركات الصغيرة الأقل حظاً) الاستفادة من موارد تقنية المعلومات ومن توجيه أعضاء هيئة التدريس المحليين بكتابة مقترحات الأعمال، والتسويق والتوزيع وغيرها[٢٩].

أما المكتبة فهي صغيرة لكنها نشطة جداً. وبالإضافة إلى خدمات المكتبة التقليدية تقدم المكتبة الدرجات الجامعية ودرجات الدراسات العليا في علوم المكتبات. وتبحث المكتبة بشكل نشط عن شراكات مع البائعين والناشرين من أجل التحول إلى النموذج الإلكتروني للكتاب الجامعي. كما تقوم بمجهود كبير لدمج المجموعات المكتبية الحكومية والمحلية، وتحسين نظم الإعارة بين المكتبات.

وتقوم إدارة خدمات الطلاب بتلبية احتياجات الطلاب اللاصفية مثل القروض الطلابية، والإسكان، والقوانين الأخلاقية، والحكومة الطلابية، وغيرها من التنظيمات الطلابية الأخرى.

(٢٩) من ويكيبيديا: (الشركات الصغيرة الأقل حظاً) هي شركة صغيرة يملك ما لا يقل من ٥١٪ منها شخص أو أكثر من المُصنفين على أنهم محرومون اجتماعياً واقتصادياً. واندراج الشركة تحت هذا المسمى يجعلها مؤهلة لمزايا العقود والمناقصات التابعة لبرامج المشتريات الفدرالية.

وتتميــز إدارة خدمات المال والأعــمال إلى حد كبير بالمركزية. وتتــولى إدارة الخدمات الإدارية ما يلي: المشتريات، والعيادة الصحية الجامعية، وخدمات الصيانة، وشرطة الجامعة. كما أنها تتعامل مع الرواتب، وإجراءات التوظيف، ومســتحقات الموظفين. وتتعامل إدارة تقنية المعلومات مع كل جهود تقنية المعلومات على مستوى المنظمة، متضمناً ذلك أنظمة إدارة أعــمال المنظمــة (Enterprise Business Systems). أمــا نظام معلومات الطالب، ونظام الموارد البشرية، ونظام الرواتب والمالية فكلها مُشغلة بطريقة مركزية.

ويتم تشــغيل بعض خدمات تقنية المعلومات الإضافية بالمزج بين الخدمات المركزية والدعم المحــلي. وتشــمل هذه الخدمــات: إدارة ودعم ســطح المكتب، إدارة مشــاركة الملفات، إدارة الطباعة، وتوفير الحسابات، وإدارة أجهزة الخادم. ولتوفير التكاليف يقوم أعضاء هيئة التدريس غير الدائمين، والمســؤولين بشــكل رئيسي عن تدريس المقررات الدراسية، بإدارة هذه الخدمات. وبصفة عام فإن الفريق الفني يعمل لساعات طويلة مقابل أجر مالي قليل لكنه مؤهل ومُدرب بشــكل جيد بحيــث يبذل هذا الفريق قصــارى جهده لتلبية توقعات الطــلاب على الرغم من محدودية الميزانية. وتجدر الإشارة إلى أن أمن المعلومات جزء من إدارة تقنية المعلومات.

أسئلة على تصميم الحالة الأمنية:

أجب عن الأسئلة التالية فيما يتعلق بجامعة ولاية الشمس المشرقة:

١. ما هي بعض الطرق التي من الممكن أن تسبب الارتباك أو الخسائر المالية للجامعة بسبب ثغرات أمن المعلومات؟

٢. اذكــر ثلاثة من المعلومات المُخزنــة في نظم معلومات الجامعة والتي من المُتوقع أن تحافــظ الجامعة عــلى خصوصيتها؟ ما هي بعض الطرق التــي يُمكن أن تؤدي إلى انتهاك خصوصية كل عنصر من هذه العناصر الثلاثة؟

٣. اذكــر ثلاثة من المعلومات المُخزنــة في نظم معلومات الجامعة والتي من المُتوقع أن تحافــظ الجامعــة على تكاملها؟ ما هــي بعض الطرق التي يُمكن أن تؤثر ســلباً في تكامل كل عنصر من هذه العناصر الثلاثة؟

٤. اذكــر ثلاثة من المعلومات المُخزنــة في نظم معلومات الجامعة والتي من المُتوقع أن تحافــظ الجامعة على جاهزيتها؟ ما هي بعض الطرق التي يُمكن أن تؤثر ســلباً في جاهزية كل عنصر من هذه العناصر الثلاثة؟

الفصل الثاني

إدارة النظام (الجزء الأول)

نظرة عامة:

كــما ذكرنا في الفصــل الأول أن الهدف من أمن المعلومات هو حماية المعلومات وكذلك حمايــة نظم المعلومات من خلال ضــمان خصوصية المعلومات وتكاملها وجاهزيتها. ولقد ناقشــنا بعض الأمثلة لكيفية اختراق أمن المعلومات، كما ناقشــنا النتائج المترتبة على مثل تلك الانتهاكات. ومن الواضح أن الشركات تسعى لحماية نفسها وحماية عملائها. لذا كيف يمكن أن نفعل ذلك؟ بقية هذا الكتاب مخصص للإجابة فقط عن هذا السؤال. هذا الفصل يطــرح موضوع إدارة الأنظمة وهو أحد المكونات الأساســية لتعامل المنظمات مع مخاوف أمن المعلومات. في نهاية هذا الفصل يجب أن تعرف:

- ماهية إدارة النظام.
- الأسباب التي تجعل من إدارة النظام موضوعاً مهماً لأمن المعلومات.
- المــوارد العامة لإدارة النظام والتــي يمكن الحصول عليها مــن أنظمة برمجيات المؤسسة.

مقدمة:

تتكون الاســتجابة الشــاملة لأمن المعلومات في المنظمة من العديد من المكونات بما في ذلك الإجراءات القياسية، وتدريب المســتخدمين، والمساءلة الإدارية. وسنقوم بتناول هذه الموضوعات بالترتيب المناسب في هذا الكتاب. لكن خط الدفاع الأول هو الجهد المبذول من قبل مسؤولي النُظم لحماية أنظمة المعلومات الهامة. مسؤول النظام هو الشخص المسؤول عن العمليات اليومية للأنظمة التقنية[1].

---

(1) ATIS Telecom glossary: http://www.atis.orglglossary/default.aspx

ونظـراً لأهمية أمن المعلومات للعمليات اليومية للأنظمة التقنية فإن مســؤول النظام يؤدي في كثير من الأحيان دور مســؤول أمن النظام أيضاً. مسؤول أمن النظام هو الشخص المســؤول عن وضع وتطبيق ومراجعة إجراءات الأمن التشـغيلية. وتُعد وظائف مسؤولي النظم من أهم الوظائف التقنية في المنظمة.

ويقــدم هذا الفصل موضوع إدارة النظام ويشرح الأهميــة الكُبرى لهذا الموضوع لأمن المعلومات. ثم يســتعرض الفصل بعض الأمثلة للموارد القياســية لإدارة الأنظمة والمتوفرة في برمجيات المؤسســة والتي تعمل على أنظمة التشـغيل الرئيســية. وأما نشاط التمرين العمــلي في هذا الفصل فيعطيك الفرصة لتحميل وتثبيت وضبط النســخة الخاصة بك من نظام التشغيل لينكس (Linux). ونظام التشغيل هذا تم تخصيصه من قِبَل مؤلفي الكتاب ليشمل إصدارات الأدوات المساعدة لأمن المعلومات الأكثر شيوعاً لدى مسؤولي النظم. وتم اختبار تلك الإصدارات من قِبَل مؤلفي الكتاب. وســيتم اســتخدام هذه الأدوات المساعدة أيضاً في الأنشــطة العمليــة في الفصول اللاحقة. ويتضمن نظام التشــغيل محاكاة مصغرة لجامعة ولاية الشــمس المشرقة والتي ستكون مفيدة في الحالة المترابطة بجميع موضوعات فصول الكتاب والتي تكلمنا عنها سابقاً.

لماذا نســتعرض موضوع إدارة النظام في بداية هذا الكتاب؟ ولماذا نركز على أنشــطة التدريب العملي المتعلقة بإدارة النظم؟

إدارة النظــام الفعالــة تتطلب قدراً كبيراً مــن الانضباط والمهارة الفنيــة، وتطوير هذه المهارات يســتغرق وقتاً طويلاً. ومــن المُغري أن نقوم بترحيل موضــوع إدارة الأنظمة إلى ملحقات الكتاب، أو أن نوجه الطلاب إلى مصادر على الإنترنت لتطوير هذه المهارات. لكننا نعتقــد أن إدارة النظام مهارة أساســية يحتاجها متخصصو أمن المعلومات الطموحون. لذا فإننا نســتعرض هذا الموضوع في بداية هذا الكتاب. وســوف نســتخدم أنشــطة التدريب العملي بعد كل فصل لمســاعدتك في صقل مهارات إدارة النظام والمهارات الفنية. ويعتقد كثير من الطلاب بأن أنشطة التدريب العملي هي العنصر الأكثر قيمة في هذا المقرر الدراسي. ويثمن العديد من مسؤولي المنظمات هذه المهارات أيضاً خصوصاً للموظفين المبتدئين.

ما هي إدارة النظام؟

إدارة النظــام هي مجموعة من الوظائف التي توفــر خدمات الدعم، وتضمن الثقة في العمليات، وتعزز الاستخدام الفعال للنظام، وتضمن تحقيق أهداف جودة الخدمة المحددة. وتشــمل إدارة النظام: تثبيــت وضبط وصيانة معدات الشــبكات (المحولات، والموجهات، وبروتوكــول التكوين الديناميكي DHCP، وخوادم نظام تحديد العناوين الشــبكية DNS Servers وغيرها) وأنظمة الحاسب الآلي (أنظمة قواعد البيانات، وأنظمة البريد الإلكتروني، وأنظمــة تخطيط المــوارد ERP systems وغيرها). واعتماداً على حجــم وتعقيد الأنظمة المعنية فإن الوقت اللازم لتوفير هذه الخدمات يتراوح بين جزء بسيط من الوقت الأسبوعي لموظــف واحد من تقنيــة المعلومات إلى الوقــت الكامل لفريق متخصص من المســؤولين والمبرمجين وموظفي الدعم. وإذا قمت في السابق بتثبيت برنامج جديد أو استبدال قطعة لا تعمل في جهازك فإنك قد قمت بوظيفة مســؤول النظام وإن كان ذلك على نطاق ضيق. وعــلى الطرف الآخر توظف شركات مثل شركة جوجل الآلاف من مســؤولي النظم وغيرهم من الموظفين لدعم مئات الآلاف من أجهزة الحاســب الآلي[٢]. وعندما تكون أنظمة العمل الهامة خارج الخدمة يعني ذلك خســارة في العوائد تُقدر بــآلاف وأحياناً ملايين الدولارات في كل دقيقة من الزمن، لذلك فإن مســؤولي النظم ذوي المهارات العالية مرغوب فيهم في هذه الصناعة.

اتجاهات ذات صلة - الحوسبة السحابية:

واستجابة لتعقيدات إدارة النظام، ظهر في السنوات الأخيرة اتجاهان حديثين للتكنولوجيا. وكل من هذين الاتجاهين يندرج تحت فئة الحوســبة الســحابية. والحوســبة الســحابية هــي تقديــم البرامج وغيرها من موارد الحاســب الآلي عبر الإنترنــت كخدمة وليس كمنتج منفصــل[٣]. والاتجاه الأول هو البرمجيات كخدمــة (Software as a Service)، وهي آلية لتســليم البرمجيات يتم فيها توفير التطبيقات وجميع الموارد المرتبطة بها إلى المنظمات عن

---

(2) http://www.dalacenterknowledge.com/archives/2011/08/01/report- google-uses-about-900000-servers/

(3) http://en. wikipedia.org/wikilCloud_computing

طريــق مُورِد البرمجيات كخدمة وتتم من خلال متصفح الإنترنت. ويقوم مُورِد (البرمجيات كخدمــة) بتوفير جميع مكونــات الأجهزة والبرمجيات ويأخذ على عاتقه مســؤولية جميع جوانب إدارة النظام. وسعر هذه الخدمة يكون على شكل اشتراك مع تكلفة مدفوعة لكل مســتخدم على أســاس شهري أو ســنوي. ويتم توفير بعض تطبيقات (البرمجيات كخدمة) مجانــاً ويتم الحصول عــلى العائد المادي من الإعلانات التجارية. وإذا اســتخدمت أياً من التطبيقات على شــبكة الإنترنت كمحرر مستندات جوجل (Google Docs) أو استخدمت خدمــة حفظ الملفات على الإنترنت مثل دروب بوكس (DropBox) فإنك قد اســتخدمت تطبيقات (البرمجيات كخدمة).

الاتجــاه الثاني هو البنية التحتية كخدمــة (Infrastructure as a Service). و(البنية التحتية كخدمة) هي نموذج أعمال تقوم المنظمات من خلاله باســتخدام معدات ومكونات الأجهــزة كالمعالجات والتخزين وأجهزة التوجيه من مُــورِد (البنية التحتية كخدمة). وتُعد (البنية التحتية كخدمة) من أشــكال الحوســبة الســحابية أيضاً. وخلافاً لمُــورِد البرمجيات كخدمة، فإن مُورِد (البنية التحتية كخدمة) يوفر مكونات الأجهزة ويتحمل فقط مســؤولية تركيب الأجهزة والصيانة. ويجب أن تُنفذ جميع عمليات أنظمة التشغيل وإدارة التطبيقات من خلال مســؤولي الأنظمة في المنظمة. ويكون الســعر على أســاس الاشتراك وعلى أساس الاســتخدام (مثلاً الحفظ لكل قيقا بايت، وعدد دورات وحدة المعالجة المركزية لكل مليون دورة). ومــن الشركات المعروفة في تقديم (البنيــة التحتية كخدمة) شركة أمازون[٤] وشركة راك سبيس[٥].

بدأ مســؤولو النظم في الســنوات الأخيرة بنشر تقنية تُسمى الآلات الافتراضية (virtual machines) بهدف زيادة كفاءة استخدام قطع أجهزة الحاسب الآلي. والآلة الافتراضية هي وعــاء للبرمجيات يمكن أن يُثبَت فيه أي نظام للتشــغيل وأي نوع من التطبيقات. وتعمل الآلات الافتراضية تماماً مثل نظائرها المادية لكن دون إمكانية فشل مكونات أجهزة الحاسب الآلي. ويمكن تشغيل وإيقاف الآلات الافتراضية عند الطلب. مثلاً يمكن تشغيل آلة افتراضية جديدة لتقوم بوظيفة خوادم الشبكة (Web Servers) وذلك في أوقات ذروة العمل (مثل

(4) http://aws.amazon.com/

(5) https://www.rackspace.com/cloud

موسم الإجازات لتاجر ما على الإنترنت). وبمجرد انتهاء موسم الإجازة ورجوع معدل العمل لمستواه الطبيعي، يمكن إزالة تلك الخوادم الافتراضية الإضافية. ومثالاً على فائدة الآلات الافتراضية ستقوم في نشاط التدريب العملي في نهاية هذا الفصل بإنشاء آلتك الافتراضية، كما ستقوم باستخدامها في معظم الأنشطة العملية المُتبقية في هذا الكتاب. وعندما تتعاقد المنظمة مع مُورِد (بنية تحتية كخدمة) فإن المنظمة تشتري إذن استخدام الآلة الافتراضية.

وتستطيع المنظمات أن تدفع فقط لعدد محدود من الخوادم التي تحتاج إليها في الوقت الذي تحتاج إليها فيه، وذلك عند الجمع بين البنية التحتية كخدمة والآلات الافتراضية، بدلاً من شراء وصيانة خوادم فعلية تكفي للتعامل مع ذروة العمل.

إدارة النظام وأمن المعلومات:

قد تتساءل بينك وبين نفسك عن العلاقة بين إدارة النظام وأمن المعلومات. في الواقع إن إدارة النظام هي خط الدفاع الأول عن الأبعاد الثلاثة لأمن المعلومات: الخصوصية، والتكامل، والجاهزية. تأمل في جاهزية المعلومات. إذا كانت معلومات هامة، كدرجاتك الدراسية، غير متوفرة بسبب فشل الخادم الذي تم تخزين الدرجات فيه ولم يكن هناك وسيلة لاستردادها، فإنك تتأثر بشكل مباشر بفشل مسؤول النظام. إن توقع مثل هذه المشكلات تقع على عاتق مسؤول النظام، كما أنه مسؤول عن استخدام الأساليب المناسبة لمنع فشل الأجهزة من التأثير في المستخدمين النهائيين. ويقضي مسؤولو الأنظمة مُعظم وقتهم في التخطيط لإصلاح واسترداد أعطال الأجهزة. وكمثال آخر تأمل في الخصوصية. ماذا لو أن معلومات هامة، ككشف الدرجات الخاص بك، سُرقت من أنظمة الجامعة ووضعت على صفحات الإنترنت ليراها كل شخص؟ هذا سيكون أيضاً فشلاً لإدارة الأنظمة. إن توقع مثل هذه المشكلات تقع على عاتق مسؤول النظام، كما أنه مسؤول عن استخدام أذونات الملف المناسبة لضمان أن الأشخاص غير المصرح لهم لا يمكنهم من قراءة أو نسخ كشف الدرجات.

وكما ترى فإن كل شيء يفعله مسؤولو الأنظمة يكون ذا علاقة بأمن المعلومات، ومعظم الجوانب الفنية لأمن المعلومات يمكن معالجتها من قِبَل مسؤولي الأنظمة. ويوضح القسم

التالي بعض المهام الشائعة التي يقوم بها مسؤولو الأنظمة. كما يوضح القسم الذي يليه بعض الأدوات الشائعة التي توفرها أنظمة برمجيات المؤسسة لمساعدة مسؤولي الأنظمة في تنفيذ هذه المهام.

المهام الشائعة لمسؤولي النظام(٦):

كل مرحلة من مراحل استخدام التقنية تتضمن مهام لإدارة الأنظمة. وتشمل هذه المهام تثبيت وضبط الأنظمة حتى يمكن استخدامها، والتحكم في الوصول وإدارة المستخدمين بحيث يتمكن المستخدم من العثور على ما يحتاج إليه دون التسبب سهواً بإحداث ضرر للنظام، والرقابة المستمرة على النظام لضمان أن كافة المكونات تعمل كما هو متوقع، وتطبيق التحديثات وبالأخص عندما تكشف المراقبة عن مشكلات ذات صلة بالأداء والأمن.

التثبيت والضبط:

التثبيت هو كتابة البيانات اللازمة في المكان المناسب على القرص الصلب لجهاز الحاسب الآلي بهدف تشغيل البرنامج. المهمة الأولى لإعداد جهاز حاسب آلي جديد هي تثبيت نظام التشغيل. وإذا قمت في السابق بتثبيت نسخة من نظام تشغيل مايكروسوفت ويندوز (Windows) أو توزيع نظام لينكس (Linux) فإن عملية التثبيت مألوفة بالنسبة لك، وهي تبدأ بتشغيل جهاز الحاسب الآلي مع قرص التثبيت، ثم تجيب عن بعض أسئلة الضبط، وتختار القرص الصلب الذي سيتم تثبيت نظام التشغيل فيه، وتختار البرمجيات وهي ستُثبتها، ومن ثم تنتظر حتى يتم نقل الملفات. وخطوات تثبيت متشابهة جداً بغض النظر عن نظام التشغيل الذي تقوم بتثبيته. وبينما يكون تثبيت وضبط البرمجيات لجهاز واحد عملية واضحة تماماً، يكمُن التحدي الأكبر لمسؤولي الأنظمة في تبسيط إجراء هذه العملية لمئات أو آلاف من أجهزة الحاسب الآلي في المنظمة. وفي القسم التالي سنقدم لمحة عامة عن بعض الأدوات الشائعة الاستخدام للقيام بهذه المهام.

الضبط هو اختيار مجموعة مواصفات النظام من بين المجموعات الممكنة. وللضبط تأثيرات عدة على أمن المعلومات. ويمكن أن يؤسس الضبط المعقد مواطناً للضعف بسبب

---

(٦) مصادر قصاصة البريد المزعج:

I. Morozov. E. ‹The common enemy,» WSJ Book Review. May 9, 2013.

2. Brunton. F. «Sparn: a shadow history of the Internet (infrastructures),» MIT Press. ISBN 026201 887X.

التفاعـل بين المكونات المختلفة، وعدم قدرة مسـؤولي الأنظمة على فهم الآثار المترتبة على هـذا التفاعـل. كما لا يتم الحفاظ على العديد من مكونـات البرمجيات المرغوب فيها مما يؤدي إلى مخاطر في أمن المعلومات. ولهذه الأسـباب فـإن القاعدة العامة بين خبراء إدارة الأنظمة فيما يتعلق بالضبط تنص على «عندما تشك لا تقم بالتثبيت». في حين أن القاعدة العامة بين المستهلكين تنص على «عندما تشك قم بالتثبيت أو التحديث».

يُنسب لشـخص يُدعى بيتر بوس، وهو مهندس في معهد ماساتشوستس للتقنية، أنه أول من اسـتخدم امتيازاته كمسؤول للنظام لإرسال أول رسـالة إلكترونية مزعجة (spam message) في العالم في عام ١٩٧١. وقام بتوجيه الرسالة إلى نحو ألف شخص من زملائه المهندسين متضمناً ذلك وزارة الدفاع الأمريكية.

كان الهدف من أول رسالة إلكترونية مزعجة في العالم هو:

أ. بيع أجهزة حاسب آلي مستخدمة

ب. معارضة حرب فيتنام

ج. البحث عن وظيفة

د. توظيف طلاب في المختبر

(الإجابة في الصفحة التالية)

التحكم في الوصول وإدارة المستخدمين:

التحكـم في الوصول هو تقييد الوصـول إلى موارد نظم المعلومات للمصرح لهم فقط من المسـتخدمين والبرامج والعمليات والنظم. ويحدد التحكم في الوصول ما يمكن للمستخدمين القيام به على النظام. وعادة يشير التحكم في الوصول إلى الملفات والأدلة التي يمكن للمستخدم أن يقرأها أو يعدلها أو يحذفها، لكن في بعض أنظمة التشغيل فإن الوصول إلى منافذ الشبكة وغيرها من مسـتويات نظام التشـغيل الهيكلية يمكن تحديده أيضاً. ويمكن تطبيق التحكم في الوصـول على مسـتوى التطبيق حيث يمكـن تحديد الصفوف و/أو الأعمـدة التي يمكن للمستخدم رؤيتها في قاعدة البيانات أو تحديد الشاشات المتوفرة في تطبيقات الأعمال.

وتُعـد إدارة المسـتخدم مـن المكونات الأساسـية للتحكم في الوصـول. ويُقصد بإدارة المسـتخدم تحديد حقوق أعضاء المنظمـة فيما يتعلق بالمعلومات الموجـودة في المنظمة. وعلى الأرجح أن إنشـاء حسـابات المسـتخدمين وإلغاءها هو أول ما يفكر به الناس عند سـماعهم لمصطلح «إدارة المستخدم». ومن الشائع عند إدارة أعداد كبيرة من المستخدمين أن يتـم تنظيمهم في مجموعات بامتيازات متماثلة. على سـبيل المثـال فإن جميع أعضاء هيئة التدريس في قسم علوم الحاسب الآلي يمكن جعلهم في مجموعة يطلق عليها مجموعة (Compsci-Faculty). ويمكـن أن تُمنـح هـذه المجموعة الوصول إلى مـوارد معينة على الموقع الإلكتروني للقسم أو تكون كقائمة بريد تُستخدم لمناقشات البريد الإلكتروني.

العلاقـة بين كل مـن التحكم في الوصول، وإدارة المسـتخدم، وبُعـدَي أمن المعلومات (الخصوصية والتكامل) علاقة واضحة ومباشرة حيث يقوم مسؤول النظام بتأسيس التحكم في الوصول لمجموعة من المعلومات لضمان أن السماح يتم فقط للمستخدمين المصرح لهم لرؤية (خصوصية) أو تعديل (تكامل) معلوماتهم. ويمكن أن تكون هذه العملية بسـيطة لكـن حجم المنظمة، وكمية البيانات، ومدى التعقيد وفرص حدوث الأخطاء تزداد بشـكل كبير. وسنتطرق إلى هذه القضايا بعمق أكبر في الفصل السابع.

الرقابة والفحص:

وبمجرد تثبيت وضبط وتشـغيل النظـام فإنه يحتاج إلى مراقبة مسـتمرة لضمان الأداء والأمن المنشود. والرقابة هي الاستماع و/أو تسجيل لأنشطة النظام بهدف الحفاظ على الأداء والأمـن. وتُصنف مهام إدارة النظام في هذه الفئـة إلى نوعين: مراقبة تفاعلية (reactive)، ومراقبة اسـتباقية (proactive). المراقبة التفاعلية هي كشـف وتحليل حالات الفشل بعد حدوثها. مثلاً يمكن للمسـؤولين اسـتخدام أدوات مراقبة آلية كـ (Nagios)[٧] للحصول على فكرة عامة لـ «صحة» شبكاتهم الإلكترونية من خلال الحصول على رسائل فورية بالمشكلات التي تحـدث. وبالمثل فإن أدوات إدارة السـجل (log management tools) تقوم بجمع وتحليل سـجلات النظام مـن كافة الخوادم عبر الشـبكة وتربط بين الأحـداث والخوادم. وتسـاعد أدوات الرقابة تلك مسؤولي النظم في الكشف عن الأنماط أو الأحداث غير العادية

(7) https://www.nagios.org/

والتي تُشير إلى حدوث انتهاك أمني. وفي حال حدوث انتهاك أمني يتم تحديد عدد الأنظمة المُحتمل تأثرها بهذا الانتهاك.

أما المراقبة الاستباقية فهي فحص النظام لمشكلات محددة قبل حدوثها. ومن الممارسات الشـائعة في هذا السياق استخدام ماسـحات مواطن الضعف (vulnerability scanners) للوصول إلى النظام والبحث عن الثغرات المُحتملة. ثم يتم ترتيب الثغرات حسب أولويتها ومـن ثم معالجتها بناءً على ذلك. كما أن اختبار الاختراق، والذي يُنفذ عادة من قِبل شركة أمنيـة متخصصة، يأخذ خطـوة متقدمة إلى الأمام حيث يتم فيه عملياً اسـتغلال الثغرات وتقييم المستوى الذي يمكن تحقيقه من الوصول إلى النظام.

تحديث البرمجيات:

يؤدي الاستخدام والمراقبة المستمرة للبرمجيات عادة إما إلى كشف جوانب الضعف وإما إلى كشف متطلبات جديدة. وتُستخدم تحديثات البرامج لإصلاح هذه المشكلات. وتحديث البرمجيات هو استبدال المكونات المعيبة للبرامج بمكونات أخرى خالية من تلك العيوب التي تم تحديدها. ويمكن تقسـيم تحديث البرامج إلى فئتين: تحديث نظام التشغيل وتحديث التطبيقات. تحديث نظام التشغيل هو التحديث الذي يُصلح مشكلات المكونات المنخفضة المسـتوى لبرمجيات النظام، ويتـم تطويرها وإصدارها مباشرة من مُـورِد النظام. وجميع نظم التشـغيل الحديثة تشـمل برامج تقوم بالفحص والتثبيـت الآلي للتحديثات المطلوبة دون تدخل من مسؤول النظام. أما تحديث التطبيقات فيقوم بإصلاح التطبيقات الفردية. ويتضمن تحديث التطبيقات الكثير من العمل من جانب مسـؤول النظام، وذلك لأن أغلب التطبيقـات تكون مـزودة بإضافات مطورة من موردين مختلفـين وأحياناً تكون الإضافات مطورة داخلياً في المنظمة. ولا يجري توثيق العديد من هذه التخصيصات أو فحصها بشكل جيد. وليس من السـهل التنبؤ بتأثير تحديـث التطبيقات على تلك التخصيصات. لذا فإن التحديث اليدوي غالباً يكون ضرورياً لنشر تحديث التطبيقات. وتُعد المحافظة على تحديث النظم من التحديات الكُبرى في المنظمات بسـبب السلوك غير المتوقع للتطبيقات المُثبتة في الأنظمة المُحدثة. ولهذا السـبب فإن مسؤولي النظام يقومون عادة بتثبيت التحديث على

خادم التطوير (development server)، ومن ثم اختبار جميع التطبيقات في نظام التطوير قبل نشر التحديث على نظام الإنتاج.

بيتر بوس

الإجابة: (ب)

وكان نص الرسالة «لا توجد وسيلة للسلام. السلام هو الوسيلة».

الفيسبوك، واستكشاف البريد الإلكتروني، وإدارة النظام، والقانون:

بدأ مارك زوكربيرج في تأسـيس الموقع الإلكتروني لفيسـبوك في الرابع من فبراير من عام ٢٠٠٤ عندمـا كان طالبـاً في جامعة هارفارد. ومع مرور الوقت أخـذ هذا الموقع في النمو ليُصبح الشركة المشـهورة (فيسـبوك). وعندما كان مارك طالباً في هارفارد وقبل نحو تسعة أشـهر من إطلاق فيسـبوك، وقـع مارك عقداً مـع متعهد من ريف نيويـورك يدعى باول سـيجليا، وذلك لإنشاء موقع يدعى (StreetFax). وفي عام ٢٠١٠ قدم باول سيجليا دعوى قضائية في مدينة بافالو في نيويورك يدّعي فيها أن العقد كان لتأسـيس فيسبوك ولم يكن لـ (StreetFax). ووفقاً للعقد يحق لباول الحصول على (٥٠٪) من شركة فيسـبوك. وتُشـير التقديـرات إلى أن هـذه الحصة يمكن أن تصل قيمتها إلى ٥٠ بليـون دولار وذلك في وقت الدعوى القضائية. وأحضر باول نسخة من عقده مع مارك دعماً لادعاءاته.

حسـناً ما علاقة ذلك بأمن المعلومات بشكل عام وبإدارة الأنظمة على وجه الخصوص؟ قبـل أن تقـرأ أكثر فكر للحظة في الأمور التي يمكن أن تفعلها فيسـبوك لإثبات عدم صحة ادعاءات باول (الشكل ٢-١).

أعدت فيسبوك في حركتها لرد الدعوى نتائج للبحث في خادم البريد الإلكتروني في جامعة هارفارد. ونصت حركة فيسبوك للرد على الدعوى على ما يلي: «...استعرضنا جميع رسائل البريـد الإلكتروني الخاصـة بزوكربيرج الموجودة في حسـاب بريده الإلكـتروني والذي كان يستخدمه عندما كان طالباً في جامعة هارفارد. وتضمن هذا الحساب رسائل إلكترونية من الفترة ٢٠٠٣ إلى ٢٠٠٤. واتضح أن رسـائل البريد الإلكتروني التي اقتبسـها باول سـيجليا في

شــكواه المعدلة لا وجود لها في الحساب، وهي محض افتراءات.... وقمنا بالبحث في جميع رســائل البريد الإلكتروني الموجودة في الحساب باستخدام عبارات بحث تحتوي على كلمات من رسائل البريد الإلكتروني المزعومة والمقتبسة في شكوى باول سيجليا المُحرفة... ولا وجود لرســائل البريد الإلكتروني المزعومة في حســاب البريد الإلكتروني لزوكربيرج. ولا وجود حتى لرســالة إلكترونية واحدة على خادم البريد الإلكتروني لهارفارد. ويُوجد في حســاب هارفارد العديد من رســائل البريد الإلكترونية بين زوكربيرج وســيجليا وموظفي شركة (StreetFax) والتي تحتوي على فشــل ســيجليا في دفع المبالغ المستحقة لزوكربيرج مقابل عمله في شركة (StreetFax). كما تحتوي على أعذار سيجليا المتكررة وطلبه السماح من زوكربيرج ووعود سيجليا بصرف المبلغ المستحق لزوكربيرج. وتوضح الرسائل الإلكترونية الحقيقية في حساب زوكربــيرج أنــه لم يناقش مطلقاً موضوع الفيســبوك أو أي موقــع للتواصل الاجتماعي مع ســيجليا أو زملائه. وقصة سيجليا أن هناك شراكة مزعومة مع زوكربيرج لإطلاق الفيسبوك هي محض خيال.

تفاصيل الموضوع موجودة في مقال في مجلة (Wired Magazine) وهو مقال يســتحق القراءة للمهتمين بهذا الموضوع.

الشكل (٢-١): باول سيجليا



المراجع:

1.Paul D. Ceglia vs. Mark Elliott Zuckerberg, “Memorandum of law in support of defendant’s motion to dismiss,” March 26, 2012.

2. Raice, S. “A Facebook founder fight,” Wall Street Journal, March 27, 2012, B7.

3. Kravets, D. “How forensics claims Facebook ownership contract is ‘forged’,” Wired Magazine, March 27, 2012, http://www.wired.comlthreatlevel/2012103/facebook-ownership-forensics/ (accessed 07/23/2013).

نقاط العطل المفردة:

ما هو أقدم بريد إلكتروني في كل حسابات البريد الإلكتروني التي تمتلكها؟

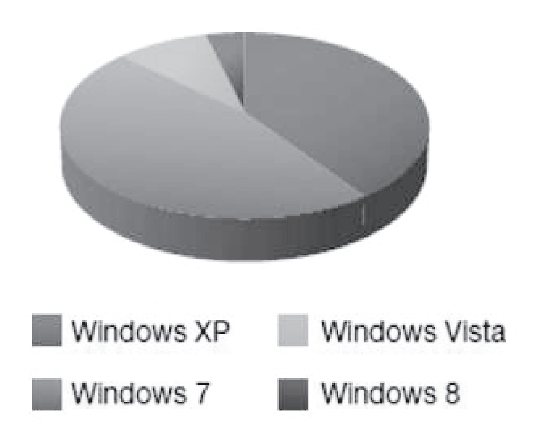
ما هو موضوع ذلك البريد الإلكتروني؟

فيما سبق وضحنا الأنشطة القياسية لإدارة الأنظمة المتعلقة بالبرمجيات التي لها أثر في أمن المعلومات. بالإضافة إلى ذلك هناك نشاط هام لإدارة الأنظمة له صلة بالأجهزة التي لها تأثير على أمن المعلومات. بالتحديد له علاقة بنقطة العطل المفردة وهي جزء من النظام إذا تعطل يؤدي إلى توقف النظام بأكمله[٨]. وتؤثر نقاط العطل المفردة في الجاهزية. على سبيل المثال أحد نقاط العطل المفردة والشائعة في أجهزة الحاسب الآلي المكتبية هو التيار الكهربائي الذي إذا انقطع فإن أجهزة الحاسب الآلي لا تتمكن من العمل حتى يتم تثبيت بديل للتيار الكهربائي. والحل القياسي للتعامل مع مشكلات نقاط العطل المفردة هو توفير قطع احتياطية (Redundancy). وتوفير القطع الاحتياطية يعني توفير إمكانيات إضافية يتم المحافظة عليها لتحسين موثوقية النظام. على سبيل المثال يمكن الاحتفاظ بمصدر طاقة احتياطي جاهز للتثبيت في حال احتياجه، وذلك لتقليل وقت التوقف عن العمل. وتُعرف هذه الأجزاء الاحتياطية بالقطع الاحتياطية الباردة، وتكون مفيدة لتقليل وقت التوقف عن العمل. لكن ومع ذلك سيكون هناك بعض الوقت الذي يكون فيه النظام غير متوفراً. ومعظم خوادم الحاسب الآلي الكبيرة تستخدم القطع الاحتياطية الساخنة وهي

(8) https://en.wikipedia.org/wiki/Single_point_of_failure

المكونات الاحتياطية التي تستقر داخل الخادم وتَحِل محل الأجزاء المتعطلة دون حدوث أي تعطل في العمل. وتسمح المكونات الاحتياطية كذلك لمسؤولي الأنظمة التعامل مع الأعطال الخارجية. على سبيل المثال، تسمح البطارية الاحتياطية لمسؤولي الأنظمة التعامل مع مشكلات انقطاع التيار الكهربائي (الشكل ٢-٢).

الشكل (٢-٢): استخدام أجهزة الحاسب الآلي المكتبية لأنظمة ويندوز-أبريل ٢٠١٣



أدوات إدارة النظام:

ونظراً للدور الهام لإدارة النظام في المنظمة، وكذلك للأهمية العالية لوقت مسؤول النظام، تطور مع مرور الوقت العديد من أدوات إدارة النظام المتخصصة في برمجيات وأجهزة المنظمة. ونقدم في هذا القسم لمحة عامة عن الأدوات الشائعة في إدارة النظام المستخدمة لنظم التشغيل السائدة: نظام تشغيل ويندوز ونظام تشغيل لينكس/ينكس. وتتوفر أيضاً أدوات مماثلة لإدارة النظام في المنظمات كقواعد البيانات والموجهات والأجهزة. وفي البداية سنلقي نظرة على الملامح العامة لهذين النوعين من نظم التشغيل ومن ثم سنلقي نظرة على بعض أدوات إدارة النظام الشائعة لهذين النظامين.

مايكروسوفت ويندوز:

في شــهر أبريل من عام ٢٠١٣ بلغت الحصة الســوقية لمايكروسوفت ويندوز (٩٢٪) من ســوق أجهزة الحاســب الآلي المكتبية[٩]. مما يعني أنك إذا كنت تســتخدم جهاز حاسب آلي فإنه على الأرجح يعمل بنظام تشــغيل مايكروســوفت ويندوز. ومنذ منتصف التســعينيات وعندما تم إصدار نظام التشــغيل وينــدوز ٩٥(Windows 95) وويندوز إن تي (Windows NT)[١٠]، أطلقت مايكروســوفت نوعين من إصــدارات (Windows): الأول ويندوز لأجهزة سطح المكتب، والثاني ويندوز لأجهزة الخوادم. ويشمل إصدار ويندوز لأجهزة سطح المكتب أرقام الإصدار المألوفة وهي: ويندوز ٩٥، ويندوز ٩٨، ويندوز إم إي، ويندوز إكس بي، ويندوز فيستا، ويندوز ٧، ويندوز ٨ (Windows 95, 98, ME, XP, Vista, 7, 8). كما يشمل الدعم لمجموعة واســعة من أجهزة الحاسب الآلي والأجهزة الطرفية المستخدمة في أجهزة الكمبيوتر المنزلية. وعلى الأرجح أنك استخدمت واحداً أو أكثر من هذه الإصدارات. وبعكس ذلك فإن إصدار ويندوز لأجهزة الخوادم (NT, 2000, 2003, 2008, 2008 R2, 2012) يدعم مجموعة أصغــر بكثــير من الأجهزة والطرفيــات ويركز على الأجهزة المكتبية لقطاع الأعمال وســوق أجهــزة الخوادم. لكن الفارق الأهــم في ذلك أن إصدار ويندوز لأجهزة الخوادم يضم عدداً مــن الخدمات للتحكم في الوصول وإدارة المســتخدم وهــذه الخدمات غير متوفرة لإصدار وينــدوز لأجهزة ســطح المكتب. وأهم هذه الخدمات هي خدمات مجال الدليل النشــط (Active Directory Domain Services).

الدليــل النشــط (Active Directory) هو مجموعة من التقنيــات التي توفر المركزية لإدارة المستخدم وللتحكم في الوصول لكافة الأجهزة الأعضاء في المجال نفسه. فعند تحديد عضويــة المجال يمكن تطبيق سياســة المجموعــة (Group Policies) لمســتخدمي المجال ولأجهزة الحاســب الآلي بهدف التحكم في وصول المستخدم لميزات معينة في أجهزة محددة في المنظمة. وتصف مايكروسوفت سياسية المجموعة (group policy) بأنها البنية التحتية التي تســمح بتنفيذ ترتيبات محددة للمستخدمين والأجهزة[١١]. وغالباً ما تُستخدم سياسة

(9) https://www.netmarketshare.com/

(10) http://windows.microsoft.com/en-us/windows/history

(11) https://technet.microsoft.com/en-us/library/cc779838(v=ws.10).aspx

المجموعة لتقييد بعض الإجراءات التي قد تُشكل مخاطر أمنية مُحتملة مثل تعطيل تحميل الملفات القابلة للتنفيذ أو منع الوصول إلى برامج معينة. والخادم الذي يُطبق قواعد الدليل النشــط ضمن مجال محدد يُطلق عليه مراقب المجال (Domain Controller). ويُحافظ مراقب المجال على معلومات حســابات المســتخدمين، ويوثق المســتخدمين في المجال بناءً على هذه المعلومات، ويأذن لهم بالدخول إلى موارد المجال اســتناداً إلى سياســة المجموعة. ويحتــاج كل مجال إلى مراقب واحد على الأقل لكن يمكــن إضافة أكثر من مراقب للمجال كبديل احتياطي (Redundancy).

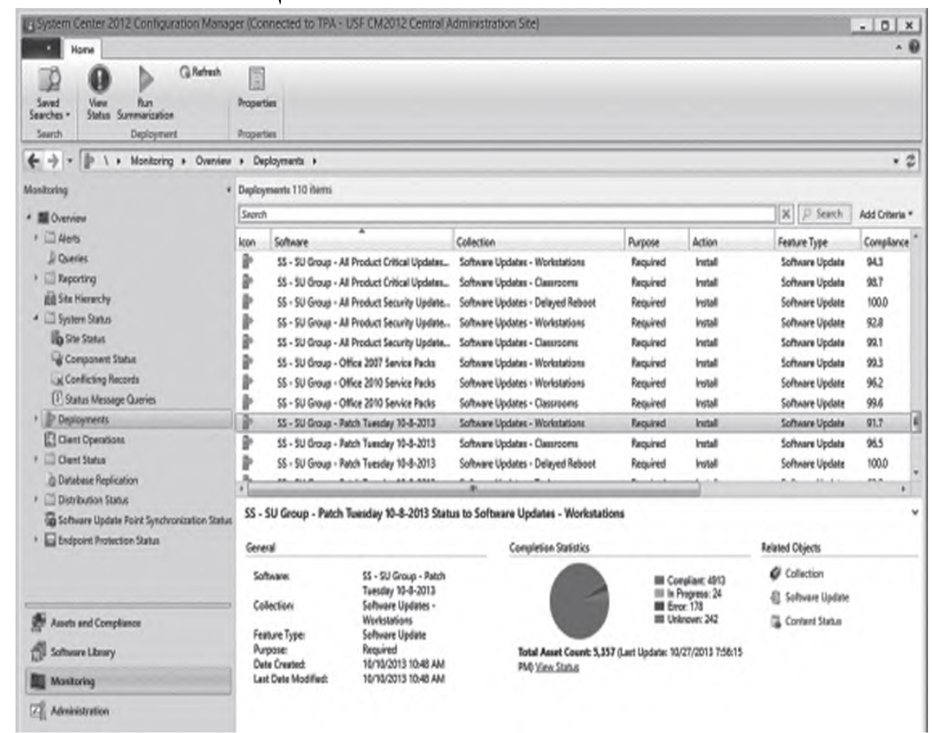
أداة إدارة النظام- مركز النظام:

تحت مُســمى مركز النظام توفر ميكروسوفت العديد من الأدوات لتثبيت وضبط نظام التشغيل ويندوز (Windows) بشكل آمن[١٢]. ويسمح مدير ضبط مركز النظام (System Center Configuration Manager) لمسؤولي النظام بإدارة عملية تثبيت نظام التشغيل وينــدوز على مئات الخــوادم والأجهزة المكتبية مــن وحدة واحدة، متضمنــاً ذلك تثبيت الخدمات والبرمجيات. وبالإضافة إلى تثبيت نظام التشغيل تقوم إدارة تكوين مركز النظام بأتمتة عملية التحديث لكل من نظام التشــغيل وحزم البرمجيات المُثبتة. وتُعطي الأدوات التــي يوفرها مركز النظام المســؤول عن النظام القدرة على نــشر البرامج الجديدة أو نشر التغييرات بشكل قابل للتكرار وقابل لجعل هذا التكرار آلياً ودقيقاً وآمناً بكل سهولة.

كما يشــمل مركز النظــام أيضاً نظام مراقبــة يُدعى مدير عمليــات مركز النظام (System Center Operations Manager) الشــكل (٢-٣) والذي يقوم بتحذير مسؤول النظام في حال تعطل الأجهزة أو حدوث أي مشكلات تؤثر في جاهزية البيانات.

(12) https://www.microsoft.com/en-us/server-cloud/system-center/

الشكل (٢-٣): مدير عمليات مركز النظام



أداة نظام التشغيل - Windows SysInternals

وللاستخدام الشخصي قد ترغب في استخدام مجموعة من الأدوات التي تقدمها مايكروسوفت وتدعــى (System Internals) والتي تعرف في مصطلحات الحاســب الآلي بـــ (SysInternals). وهــي متوفرة في الموقع الإلكتروني لميكروســوفت[١٣]. وتم تصميم هذه الأدوات لأول مرة في عام ١٩٩٦ بواســطة مارك روســنفش الذي أســس شركة (Winternals Software) والتي استحوذت عليها مايكروســوفت لاحقاً. وتعطي (SysInternals) رؤية ممتازة للأنشــطة المستمرة في جهاز الحاســب الآلي كتغيير الملفات والســجلات. وفي هذا الكتاب تم استخدام (SysInternals) لأخذ العديد من صور الشاشة (screenshots).

(١٣) عند وقت كتابة هذه الجزئية في إبريل من عام ٢٠١٢ كان الرابط هو: https://technet.microsoft.com/en-us/ aspx.sysinternals/bb٥٤٥٠٢١

ينكس/لينكس:

تم تطوير نظام التشغيل ينكس (Unix) لأول مرة تحت اسم (UNICS) في عام ١٩٦٩ مـن قبل مجموعة تابعة لمختبرات شركة آي تي آند تي (AT&T's Bell Labs) وذلك بقيادة كين طومسون ودنيس ريتشي.

حقائق متنوعة

إن تطوير نظام التشغيل ينكس يمكن أن يُنسب للعبة فيديو قديمة يُطلق عليها سبيس ترافل (Space Travel) حيث أن طومسون طور هذه اللعبة لنظام تشغيل يُدعى ملتيكس (Multics)، لكن لم يعد لدى مجموعة طومسون حق الدخول على هذا النظام ولا على الأجهزة. وأثناء عملية تطوير اللعبة على جهاز جديد تم تطوير أساس نظام التشغيل المعروف بـ (ينكس)[١٤].

في عـام ١٩٧٥ رخصت شركـة آي تي آند تي (AT&T) نظام التشـغيل ينكس لبعض المؤسسـات التعليمية والبحثية. ولأنه تم توفير الشفرة البرمجية الأصلية مع نظام التشغيل ينكـس، قامت تلك المؤسسـات بتعديل ينكس ليتـلاءم مع احتياجاتهـم. وفي عام ١٩٧٨ قامت جامعة كاليفورنيا في بيركلي بإصدار نسـخة مطورة من نظام التشـغيل ينكس تُدعى توزيعـة برمجيات بـيركلي (Berkley Software Distribution Unix). وهذه النسـخة تحتـوي على العديد من التحسـينات التي لا تزال موجودة في أنظمـة ينكس الحديثة[١٥] . وتم إطلاق العشرات من الإصدارات المتنوعة بتحسـينات خاصة لنظام ينكس اعتماداً على توزيعة برمجيات بيركلي أو على البرمجة الأصلية من آي تي آند تي. وفي عام ١٩٨٨ قامت آي تي آند تي بإصدار النسخة النهائية لنظام ينكس والتي تدعى النظام الخامس (System V)، لكن إصدارات ينكس بناء على الشـفرة البرمجية الخاصة بهم (والتي يشـار إليها بـ SysV-based Unix) ما تزال قيد التطوير إلى وقتنا الحالي[١٦]. ويوضح الشكل (٢-٤) شجرة عائلة الإصدارات الأكثر شيوعاً لنظام التشغيل ينكس.

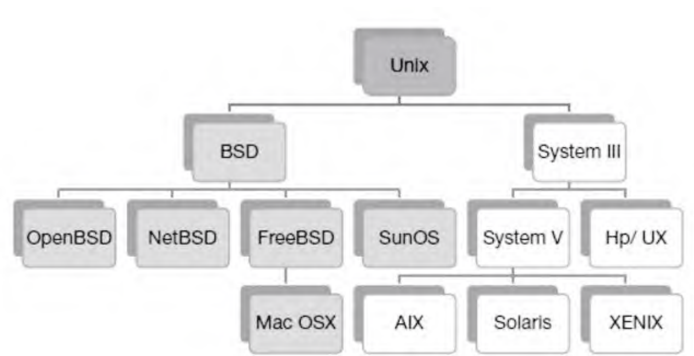
---

(14) http://www.livinginternet.com/i/iw_unix_dev.htm

(15) https://en.wikipedia.org/wiki/Berkeley_Software_Distribution

(16) https://www.levenez.com/unix/

الشكل (٢-٤): شجرة عائلة ينكس



لينكس:

في عام ١٩٩١ قام لينوس تورفالدس، وهو طالب دراسات عليا في علوم الحاسب الآلي في جامعة هلسنكي، بإصدار النسخة الأولى من نظام التشغيل الجديد المشابه لنظام ينكس ويُدعى نظام لينكس. ويُشار إلى أن نظام لينكس بأنه مشابه لنظام ينكس ليس لأنه يحتوي على أكواد برمجية من الإصدارات السابقة لنظام ينكس، بل لأنه يوفر بيئة تشمل تقريباً جميع الأدوات والمميزات الموجودة في توزيعة برمجيات بيركلي أو النظام الخامس (SysV-based Unix). وتم إصدار لينكس كأحد برمجيات المصدر المفتوح (Open Source Software). وبرمجيات المصدر المفتوح هي البرمجيات التي يستطيع أي شخص أن يعدل في شفرتها الأصلية ويقوم بنشر تعديلاته في جميع أنحاء العالم. وكان الدافع وراء تطوير قاعدة برمجيات مستقلة واعتماد نموذج ترخيص مميز هو إعطاء المطورين الفرصة لتوزيع إبداعاتهم على العالم دون عراقيل وقيود أنظمة التشغيل التجارية. وهذا التبادل الحر للأفكار تم تعزيزه بشكل كبير منذ منتصف التسعينيات وذلك من خلال زيادة الاتصال بالإنترنت. وبدلاً من أن يعمل على تطوير النظام طالب أو طالبين في إحدى الجامعات أو بضع عشرات من المطورين في شركة برمجيات تجارية، حظي نظام لينكس بعمل الآلاف من المطورين من جميع أنحاء العالم[١٧]. وخلال عقدين من إطلاق نظام لينكس تم تطوير

(17)http://www.ragibhasan.com/linux/

النظام ليعمل على كل شيء من أجهزة الحاسب الآلي العملاقة إلى أجهزة الهواتف المحمولة. ومع وجود العديد من الأجهزة التي تعمل باستخدام نظام لينكس كأجهزة تحديد المواقع، وأجهزة التوجيه اللاسلكية المنزلية، وأجهزة أندرويد، وأجهزة أمازون كيندل، من المحتمل أيضاً أن يكون لديك جهاز يعمل على نظام التشغيل لينكس. وفي شهر نوفمبر من عام ٢٠١٢ كان أسرع عشرة أجهزة حاسب آلي عملاقة تعمل على نظام التشغيل لينكس[١٨].

وما يثير الاهتمام أن عدد الإصدارات المختلفة التي جرى إنشاؤها لنظام لينكس جاءت نتيجة المرونة والطبيعة المفتوحة لنظام التشغيل حيث يستطيع كل شخص أن يُنشئ توزيع نظام لينكس الخاص به. وحالياً هناك المئات من هذه التوزيعات تحت التطوير حالياً[١٩]. وخلافاً لأنظمة التشغيل التجارية كنظام مايكروسوفت ويندوز ونظام ينكس فإنه لا يوجد نسخة رسمية لنظام لينكس لكن يوجد العديد من الإصدارات الرئيسية. وحتى الآن فإن التوزيع الرئيسي لنظام لينكس للاستخدام في بيئة الأعمال هو (Red Hat Enterprise Linux) واختصاراً (RHEL). وهذا التوزيع هو التوزيع التجاري لنظام لينكس لكن شركة رد هات (Red Hat) تُتيح الشفرة الأصلية مجاناً لنظام التشغيل بأكمله. وقد جمع مطورو مشروع سنتوس (CentOS)[٢٠] الشفرة الأصلية لنظام (RHEL) لإنشاء نظام تشغيل لينكس مجاني ومشابه لنظام (RHEL). وسوف نستخدم نسخة مخصصة من نظام سنتوس في جميع أنشطة التدريب العملي في هذا الكتاب بدءاً من نشاط التدريب العملي في نهاية هذا الفصل.

أدوات إدارة النظام:

يوجد العديد من المسميات لأدوات التثبيت والضبط التلقائية في عالم ينكس ولينكس. ومن أمثلة هذه الأدوات: (Jumpstart) في نظام (Oracle Solaris)، و(Kickstart) في نظام (RHEL)، ومدير تثبيت الشبكة (Network Installation Manager) في نظام (IBM AIX)، لكنها جميعاً تعمل بطريقة متشابهة. ويقوم مسؤول النظام بإنشاء ملف

(18) http://www.top500.org/lists/2012/11/

(19) http://distrowatch.com/search.php ?ostype=Linux&category=A 1

(20) https://www.centos.org/

يحتوي على تعليمات حول كيفية ضبط أجهزة الشـبكة والأقراص الصلبة والأجهزة الشائعة الأخـرى. كما يحتوي الملف على قائمة تضم الحزم البرامجية التي يجب تثبيتها. وأخيراً فإن الملف يحتوي على البرامج التي يجب تثبيتها لاحقاً والتي يكون عملها ضرورياً لإنهاء عملية الضبط.

وتوفر العديد من التطبيقات دعماً متعدد المنصات لتساعد على ضبط البرمجيات بعد تثبيت نظام التشغيل[٢١]. ومن بين هذه التطبيقات يُعد تطبيق (Puppet)[٢٢] التطبيق الأكثر شيوعاً حيث يُستخدم بشكل كبير من قِبل شركات الإنترنت الكبرى مثل شركة جوجل وتويتر. ويقوم مسؤول النظام بإنشاء قائمة على تطبيق (Puppet) تدعى (puppet manifest)، وتشمل هذه القائمة البرمجيات التي يجب تثبيتها والضبط المناسب لها. ومن ثم يتم إرسال القائمة (puppet manifest) إلى خادم واحد أو أكثر مما يؤدي إلى تثبيت البرمجيات بغض النظر عن نظام التشغيل الأساسي.

الملخص:

يضع هذا الفصل القاعدة الأساسية للجزء التقني من هذا المقرر الدراسي. ويؤدي مسؤولو النظم معظم الأنشطة التقنية ذات العلاقة بأمن المعلومات، ولهذا قدم هذا الفصل تعريفاً لإدارة النظام، كما وضح الدور الأساسي لمسؤولي النظم في المنظمة. كما عرض هذا الفصل أنشطة أمن المعلومات الأكثر شيوعاً والمنفذة من قبل مسؤولي الأنظمة. وأخيراً عرض هذا الفصل لمحة عامة عن الأدوات الشائعة الاستخدام في تبسيط تلك الأنشطة في المنظمات الكبيرة.

كما يضع نشاط التدريب العملي في هذا الفصل الحجر الأساس لأنشطة التدريب العملي التي ستعمل عليها في بقية فصول هذا الكتاب.

---

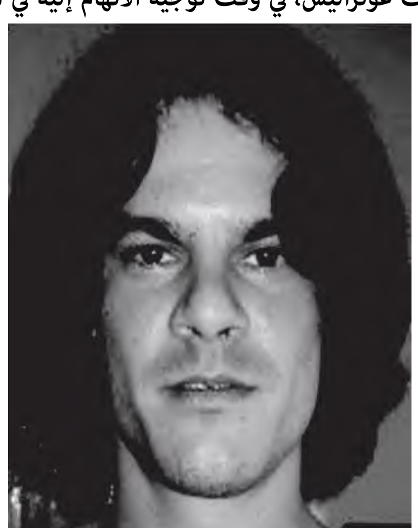
(21) https://en.wikipedia.org/wiki/Comparison_of_open-source_configuration_management_software

(22) https://projects.puppetlabs.com/projects/puppet

نموذج حالة- تي جي ماكس (T.J. MAXX):

في عام ٢٠٠٧ بدأ اهتمام الشركات بأمن المعلومات يزداد بشكل كبير وذلك بعد الكشف عن الخروقات الأمنية المُربِكة في العديد من الشركات المعروفة. وتمكن العديد من القراصنة من الوصول الكامل إلى قواعد بيانات بطاقات الدفع الائتمانية في العديد من متاجر التجزئة الرائدة بما في ذلك شركة تي جي ماكس (TJ.Maxx)، وشركة بارنس آند نوبل (Barnes and Noble)، وشركة أوفيس ماكس (Office Max) الشكل (٢-٥).

الشكل (٢-٥): ألبرت غونزاليس، في وقت توجيه الاتهام إليه في أغسطس ٢٠٠٩



وقراصنة الحاســب الآلي على علم بأنه من الأفضل أمنيــاً أن يكون القرصان خارج البلد المُســتهدف، وذلك لتجنب الملاحقة القضائية. لذا كان يُعتقد في البداية أن الهجمات كانت تأتي من قراصنة من خارج البلاد. لكن التحقيقات كشفت بأن أكثر الهجمات مصدرها محلي مما أدى إلى محاكمة ١١ رجلاً في ٥ دول متضمناً ذلك الولايات المتحدة الأمريكية. وما يُثير الاهتــمام أكثر بأن زعيــم العصابة كان مُخبراً في جهاز الخدمــة السرية في الولايات المتحدة الأمريكية.

النتيجة:

في الخامس من أغســطس من عام ٢٠٠٨ اتهمت الحكومة الأمريكية ١١ شخصاً بعدة تهم منهــا: الاحتيــال المالي الإلكتروني، وتلف أنظمة الحاســب الآلي، والتآمر، والمصــادرة الجنائية، وغيرها من التهم بسبب سرقة معلومات بطاقات الدفع الائتمانية من شركات تجزئة رائدة مثل شركة تي جي ماكس (TJ.Maxx)، وشركة نادي بي جيس هولســيل (BJ's Wholesale Club)، وشركة أوفيس ماكس (Office Max)، وشركة بارنس آند نوبل (Barnes and Noble).

وفي شــهر أغســطس من عام ٢٠٠٩ اتُّهِم العديد من أفراد العصابة نفســها مرة أخرى بسرقــة بيانات ما يقــارب ١٣٠ بطاقة دفــع ائتمانية من شركــة (Heartland Payment Systems)، وهــي الشركة التــي تعالج بيانات بطاقات الدفع الائتمانية. وإذا قلنا إن هناك ١٠٠ مليــون عائلة في الولايات المتحدة الأمريكية، فــإن هذا يعني أن هناك بطاقة ائتمانية واحــدة مسروقة لكل عائلة أمريكية. وتم توجيه لوائح الاتهام لخمســة منهم في الخامس والعشرين من شهر يوليو من عام ٢٠١٣م[٢٣]،[٢٤].

خلفية الموضوع:

تشكلت العصابة التي شاركت في جميع تلك الحوادث في عام ٢٠٠٣. وبين عامي ٢٠٠٣ و ٢٠٠٧ كانت العصابة تســتخدم طرقاً سهلة لاستغلال الثغرات الموجودة في أمن الشبكات اللاســلكية في متاجر التجزئة. ولاحظــت العصابة أنه لا يوجد في العديد من متاجر تي جي ماكس أي تدابير أمنية لشــبكاتهم اللاســلكية. ونتيجة لذلك فإن عملية الحصول على اسم المســتخدم وكلمــة السر الخاصة بالموظفين أمر ســهل حيث يتطلب ذلــك الانتظار صباحاً بأجهزة الحاسب الآلي المحمولة خارج متاجر التجزئة، ومن ثم يتم التنصت على حركة مرور الشبكة عندما يقوم الموظفون والمديرون بتسجيل الدخول إلى حساباتهم الوظيفية.

ومما يزيد الأمر ســوءاً أن لتلك الحســابات الوظيفية صلاحية الوصول إلى أنظمة تقنية المعلومات الأخرى في شركة تي جي ماكس، متضمناً ذلك الأنظمة التي تحفظ بيانات بطاقات

---

(23) http://www.justice.gov/opa/pr/2013/July/I3-crm-842.html (آخر دخول للموقع في 13/11/10)

(24)www.justice.gov/iso/opa/resources/51820137251112J7608630.pdf

الدفع الائتمانية. وباستخدام هذه المعلومات كان للقراصنة دخول مباشر على معلومات بطاقات الدفع الائتمانية. وقام أفراد العصابة لمدة عام تقريباً باستخراج البيانات وتخزينها على خوادم الشركة الخاصة ومن ثم استرجاعها في الوقت الملائم لهم. وكان هدف العصابة بيع بطاقات ائتمانية وهمية بمبالغ زهيدة.

وشكلت هذه الطريقة التي استخدمتها العصابة في هجماتها الأساس للائحة الاتهام في عام ٢٠٠٨. وبدءاً من أغسطس من عام ٢٠٠٧ قامت العصابة بتطوير مهاراتها وبدأت باستخدام هجمات حقن تعليمات الاستعلام البُنيوية (SQL injection) لتثبيت برامج ضارة على تطبيقات الشبكة وللوصول إلى قواعد بيانات الشركة. واستخدمت العصابة هذه الطريقة في هجماتها والتي جاءت في لائحة الاتهام لاحقاً في عام ٢٠٠٩.

زعيم العصابة وأنشطته:

زعيم العصابة هو ألبرت غونزاليس، وهو من سكان مدينة ميامي في ولاية فلوريدا. وبدءاً من عام ٢٠٠٣ تقريباً كان ألبرت يتجول بسيارته في منطقة ميامي بحثاً عن شبكة لا سلكية غير آمنة لأحد متاجر التجزئة باستخدام جهاز حاسبه المحمول. وتقوم محلات التجزئة عادة باستخدام هذه الشبكات لنقل معلومات بطاقات الائتمان من آلة تسجيل المدفوعات النقدية إلى خوادم شركة التجزئة. وعندما تجد العصابة شبكة مفتوحة تقوم باستخدام برنامج متلصص على الشبكة (sniffer) مُجهز خصيصاً لسحب أرقام البطاقات الائتمانية. وأحد أشهر هذه البرامج هو برنامج (Wireshark)[٢٥]، وهو برنامج مجاني وسهل الاستخدام. بعد ذلك يتم بيع أرقام هذه البطاقات الائتمانية الوهمية في السوق السوداء. وكانت الضحية الأكبر هي شركة تي جي ماكس والتي فقدت معلومات أكثر من ٤٠ مليون بطاقة ائتمانية. بعد ذلك تطورت العصابة وقامت باستخدام هجمات حقن تعليمات الاستعلام البُنيوية (SQL injection) والتي تقوم بزيارة محلات التجزئة للتعرف على أنظمة معالجة المعاملات المستخدمة في هذه الشركات. وبعد ذلك تقوم العصابة باستخدام هذه المعلومات لتحديد إستراتيجية الهجوم المناسبة لاستهداف أنظمة محددة تستخدمها تلك الشركات. كما كانت العصابة تحلل المواقع الإلكترونية لتلك الشركات بهدف

(25) https://www.wireshark.org/

معرفة تطبيقات الإنترنت المُســتخدمة، ومن ثم تضع العصابة الإستراتيجية المناسبة للهجوم على تلك المواقع.

وحصــل زعيم العصابــة ألبرت غونزاليس على أكــثر من مليون دولار كأربــاح بيع بيانات البطاقات الائتمانية. وعلى ما يبدو أنه في وقت ما قد تعطلت آلة عد الأوراق النقدية الخاصة به مما اضطره لعد مبلغ ٣٤٠,٠٠٠ دولار يدوياً كلها من فئة ٢٠ دولاراً. وفي شهر أغسطس من عام ٢٠٠٩ أقرّ ألبرت غونزاليس بأنه مذنب في الاتهامات الموجهة إليه في قضية تي جي ماكس.

في عــام ٢٠٠٣ أصبح غونزاليس مخــبراً لجهاز الخدمة السرية وذلــك بعد القبض عليه لارتكابــه جرائــم مختلفــة. وبطبيعة عمله مخــبراً في جهاز الخدمة السرية ســاعد ألبرت غونزاليس في عام ٢٠٠٤ في القبض على ٢٨ فرداً تابعين لموقع (Shadowcrew. com) والذي كان يقــوم بسرقة بيانات بطاقات الائتمان وبيعها بهدف تحقيق الأرباح. ونتيجة لعمليات هــذا الموقع غير المشروعة تمت سرقة بيانات عــشرات الآلاف من بطاقات الدفع الائتمانية. وبعد الانتهاء من عملية (Shadowcrew) بدأ ألبرت أعماله الاستغلالية.

الأثر:

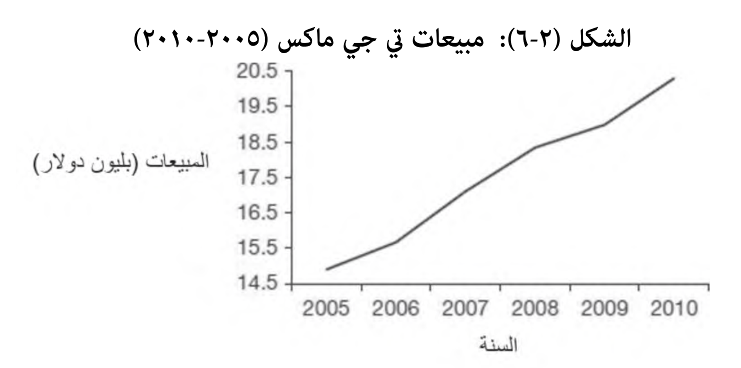
الضرر المبــاشر الناتج من هجمات الاحتيال على بطاقات الدفع الائتمانية كان محدوداً. ففي شــهر مــارس من عام ٢٠٠٧ تم القبــض على عصابة كانت تنوي اســتخدام البطاقات الائتمانيــة المسروقة من تي جي ماكــس لشراء منتجات تقارب قيمتهــا ٨ ملايين دولار من محــلات وولمارت (Wal-Marts) ومحلات نادي ســامس (Sam's Club) المتعددة في ولاية فلوريدا. لكن الأضرار الجانبية كانت جسيمة حيث اضطرت الشركة الأم وهي تي جي إكس المســاهمة (TJX Companies, Inc.)، والتي تتبع لها محلات تي جي ماكس كما تتبع لها أيضاً شركة مارشــالس (Marshalls)، لعمل تسوية قيمتها ٤٠ مليون دولار مع شركة فيزا في نوفمبر من عام ٢٠٠٧، كما عملت تسوية أخرى قيمتها ٢٤ مليون دولار مع شركة ماستركارد في أبريل من عام ٢٠٠٨.

كما جاء تأثير تلك الهجمات في كافة أنحاء البلاد حيث اضطر عشرات الملايين من العملاء إلى اســتصدار بطاقات ائتمانية جديدة. أما العملاء الذين اعتمدوا خاصية الدفع الآلي على

بطاقاتهم الائتمانية التي سُرقت فقد تلقوا إشــعارات من مقدمي الخدمات لإشــعارهم بأن المبالغ المطلوبة لم يتم خصمها بسبب إلغاء البطاقات وإصدار بطاقات جديدة بدلاً منها.

والمثير للدهشــة أن مبيعات تي جي ماكس لم تضرر بشــكل كبير كما يبدو بســبب تلك الهجمات (الشــكل ٢-٦)، فقد قامت شركات الائتمان، ومــن خلال برامج الحماية التلقائية التي تقدمها بطاقات الائتمان، بإعادة جميع الأموال للعملاء الذين تعرضت بطاقاتهم لتلك الهجمات. ويظهر من ذلك أن العملاء لا يمانعون أن تتعرض بطاقاتهم الائتمانية للسرقة إن لم يكونوا مسؤولين عن المعاملات الاحتيالية.

الشكل (٢-٦): مبيعات تي جي ماكس (٢٠٠٥-٢٠١٠)



الأهمية:

تتصــف حالة تي جي ماكس بالأهمية الخاصة لدراســة أمــن المعلومات والتخصصات الأخرى ذات العلاقة، وذلك لأن الحالة تم توثيقها في الصحافة على نطاق واسع. وبالإضافة إلى ذلــك تتوفــر تفاصيل أكثر في لوائــح الاتهام التي قُدمت في هــذه القضية. وتُمثل هذه القراءات حســاباً غنياً بالمعلومات للجهات المعنية بأمــن المعلومات، وعن دوافعهم، وعن الإجراءات القانونية المُتبعة في حوادث أمن المعلومات الكبيرة.

المراجع:

Pereira, J. “How credit-card data went out wireless door,” Wall Street Journal, May 4, 2007

Pereira, J., Levitz, J. and Singer-Vine, 1. "U.S. indicts II in global credit-card scheme." Wall Street Journal, August 6, 2008: AI.

United States of America vs.Albert Gonzalez, Criminal indictment in US District Court, Massachusetts, August 5,2008(the T.J. Maxxcase).

United States of America vs. Albert Gonzalez, Criminal indictment in US District Court, New Jersey, August 17.2009 (the Heartland case).

Zener, K. "TJX Hacker was awash in cash; his penniless coder faces prison," Wired, June 18,2009

Gorman, S. "Arrest in Epic Cyber Swindle," Wall Street Journal, August 18,2009.

Gorman, S. "Hacker sentenced to 20 years in massive data theft," Wall Street JauTl/ al. 2010: A I.

"Albert Gonzalez," Wikipedia, http://en.wikipedia.org/wikil Albert_Gonzalez. T.J. Maxx. 10-Kreports, 2006-2010. T.J. Maxx, 8-K filing, January 18,2007; April 2, 2008; November 30,2007.

أسئلة مراجعة للفصل:

١. ما هي إدارة الأنظمة؟

٢. لماذا تتصف إدارة الأنظمة بالأهمية؟

٣. من هو مسؤول النظام؟

٤. ما الأنشطة اليومية المهمة التي يقوم بها مسؤول النظام؟

٥. عرّف البنية التحتية كخدمة (Infrastructure as a Service)؟

٦. ما فوائد استخدام البنية التحتية كخدمة (Infrastructure as a Service)؟

٧. ما الخادم الافتراضي (Virtual Server)؟

٨. ما فوائد استخدام الآلات الافتراضية؟

٩. ما دور مسؤول النظام في المحافظة في أمن المعلومات في المنظمة؟

١٠.ما هو ضبط البرمجيات؟

١١.كيف يؤثر ضبط البرمجيات في أمن المعلومات؟

١٢.عرّف التحكم في الوصول. كيف يؤثر ضعف التحكم في الوصول في أمن المعلومات؟

١٣.عرّف إدارة المستخدم. كيف تؤثر إدارة المُستخدم في أمن المعلومات؟

١٤.ما المراقبة؟ وكيف تساعد المراقبة أمن المعلومات؟

١٥.ما المراقبة التفاعلية؟ وما هي بعض الطرق الشائعة في المراقبة التفاعلية؟

١٦.ما المراقبة الاستباقية؟ وما هي بعض الطرق الشائعة في المراقبة الاستباقية؟

١٧.ما عملية تحديث النظام؟ ما التحديات التي تواجه تحديث النُظم؟ ما أهمية تحديث النُظم بالنسبة لأمن المعلومات؟

١٨.ما نقطة العطل المفردة؟ وكيف يتعامل مسؤول النظام مع هذا النوع من العطل؟

١٩.ما الفرق بين القطع الاحتياطية الباردة والقطع الاحتياطية الساخنة؟

٢٠.ما الدليل النشط؟ ما الدور الذي يلعبه في المحافظة على أمن المعلومات في أجهزة الويندوز؟

٢١.ما سياسة المجموعة (Group Policies)؟ وكيف تساعد سياسة المجموعة مسؤول النظام في الحفاظ على أمن المعلومات؟

٢٢.ما مراقبة المجال؟

٢٣.اشرح بشكل مختصر (في جملتين إلى ثلاث جمل) مواصفات أمن المعلومات للإصدار الأخير من مركز النظام الخاص بمايكروسوفت أو مُنتج آخر مشابه له.

٢٤.ما هو لينكس؟ وما سبب شيوع استخدامه؟ وما هي بعض توزيعات لينكس الرائجة الاستخدام؟

٢٥.قدّم لمحة عامة (في جملتين إلى ثلاث جمل) عن قدرات برنامج تقنية المعلومات الآلي الذي يستخدمه الكثير من مسؤولي النظم والمعروف بـ (Puppet).

أسئلة على نموذج الحالة:

١. اعتماداً عــلى المعلومات الموضحة أعلاه، اذكر بعض الأمثلــة من الحالة على انتهاك الخصوصية، والتكامل، والجاهزية.

٢. اســتناداً إلى حالة تي جــي ماكس، حدد الأخطــاء في تنفيذ الأنشــطة العامة لإدارة الأنظمة في وقت حدوث الحالة.

٣. لو كنت مســؤولاً عــن إدارة النظام في شركة تي جي ماكس، ما الذي كنت ســتفعله لتفادي وقوع الحوادث الواردة في الحالة؟

نشاط التدريب العملي - تثبيت نظام لينكس:

إخلاء مسؤولية

الأنشــطة التي أنت على وشــك إجرائها يُمكن أن تضر جهاز الحاسب الآلي الخاص بك إذا لم تُطبَق بالشكل الصحيح. ومع أنه تم بذل كل الجهد لمنع ذلك من الحدوث، يُرجــى مُلاحظة أن حمايــة البيانات على جهازك وحماية الجهاز نفســه تقع في نهاية المطاف ضمن مسؤوليتك.

من أجــل الحصول على الخبرة العملية المتعلقة بالمهارات الأساســية في أمن المعلومات وإدارة الأنظمة، يتضمن الكتاب سلســلة من أنشــطة التدريب العملي التي تستخدم نظام التشــغيل لينكس. وســوف تقوم بإنشــاء البيئة الملائمة لأنشــطة التدريب العملي في هذا الفصل. وعند الانتهاء من هذا النشاط سيكون لديك نسخة العمل الخاصة بك من سينتوس لينكس (http://centos.org) والتي سنقوم باستخدامها في هذا المقرر الدراسي. وبناءً على خبرتنــا، يرى الطلاب في نهاية المقــرر الدراسي أن الفائدة الكبرى تكمن في هذه الجزئية من المقرر، كما يعتقد الطلاب أن هذه الجزئية واحدة من الأنشــطة الأكثر إثارة خلال دراستهم الجامعية. وقد تم اختيار الضبط المُحدد في هذا التمرين لأنه يسمح بإنشاء البنية التحتية اللازمة على أي جهاز حاسب آلي تملكه. ولقد بذلنا جهداً كبيراً لجعل هذا المصدر متاحاً لك لأن هذه المهارات مطلوبة بشــكل كبير من قِبل أرباب العمل، كما أن هذه المهارات تُميزك

عن منافسيك في سوق العمل. ونأمل أن تجد هذه الأنشطة مثيرة للاهتمام وأن يكون ذلك كحماسنا لإنشاء تلك الأنشطة (الشكل ٢-٧).

شكل (٢-٧): هيكلة الآلة الافتراضية



ويتكون نشـــاط التدريب العملي لهـــذا الفصل من خطوتين: في الخطوة الأولى ســـيتم تثبيت البيئة الافتراضية المســـماة (VirtualBox). وفي الخطوة الثانية ستقوم باستخدام الـ (VirtualBox) لإنشاء آلة افتراضية تحتوي على نظام تشغيل لينكس تم ضبطه مُسبقاً.

الخطوة الأولى-تثبيت الـ (VirtualBox):

قبل أن تبدأ انتبه لمتطلبات الحد الأدنى للنظام:

- ويندوز إكس بي، ويندوز ٧، ويندوز سيرفر ٢٠٠٣، أو ويندوز سيرفر ٢٠٠٨.
- ماكنتوش أو إس إكس ١٠,٥ أو أحدث.
- ٢ جيجا بايت من الذاكرة العشوائية (RAM).
- مساحة من القرص الصلب لا تقل عن ١٠ قيقا بايت.

ويقـــوم تطبيق (VirtualBox) بإنشـــاء آلـــة افتراضية على جهاز الحاســـب الآلي، ويعد (VirtualBox) تطبيقـــاً مفتوح المصدر يمكن تثبيته عـــلى أي جهاز يعمل على معالج إنتل (Intel) أو معالـــج أي إم دي (AMD). ويمكـــن تثبيت أنظمة تشـــغيل فرعية على الآلات الافتراضية. وهكذا يمكن لجهاز ويندوز، الذي يحتوي على قوة معالج وذاكرة مناسبتين، أن

يُشغل أنظمة تشغيل متعددة. اتبع هذه الخطوات لتثبيت الـ (VirtualBox) على جهازك الشخصي. وكان يتم تحديث المنتج بشكل سريع جداً وقت كتابة هذا الكتاب، لذا فإن رقم الإصدار الخاص بك قد يختلف عن رقم الإصدار الذي يظهر هنا. وستكون في مأمن عند اتباعك لقاعدة الضبط الإدارية للمستهلكين وهي «عندما تشك قم بتثبيت الإصدار الأخير». ولمعلومات أكثر عن تطبيق (VirtualBox)، بإمكانك الاطلاع على دليل الإرشادات الخاص بـ (VirtualBox)[٢٦] وبالتحديد الفصل الأول من الدليل.

١. قم بزيارة صفحة التنزيل الإلكترونية (الشكل ٢-٨) من موقع الـ (VirtualBox) وذلك للحصول على المُثبت. وهذا الرابط يتغير باستمرار لذا من الأفضل البحث عن «تنزيل الـ (VirtualBox)» للحصول على الرابط. وتبدو الصفحة كما في الشكل التالي. قم بتنزيل المثبت المناسب للنظام الخاص بك. والإرشادات أدناه خاصة بنظام التشغيل ويندوز وهي مشابهة لإرشادات التنزيل للأنظمة الأخرى.

الشكل (٢-٨): صفحة تحميل الـ (VirtualBox)



٢. وللبدء في عملية التثبيت انقر نقراً مزدوجاً على الملف الذي تم تنزيله. ثم انقر على زر «التالي» على شاشة الترحيب (الشكل ٢-٩) لبدء عملية التثبيت.

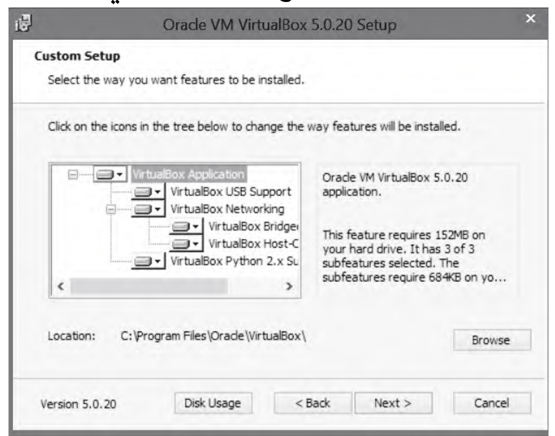
(26)http://www.virtualbox.org/manual/

الشكل (٢-٩): الصفحة الترحيبية لمُثبت الـ (VirtualBox)



٣. يُطلــب منك الآن تحديد المكان الذي ترغب فيــه لتثبيت تطبيق الـ (VirtualBox). والموقع الافتراضي هو مجلد ملفات البرامج (Program Files). انقر على زر «التالي» إذا كان موقع التثبيت الافتراضي مناسباً لك (الشكل ٢-١٠).

الشكل (٢-١٠): موقع التثبيت الافتراضي



٤. ستســتمر عملية التثبيت بشــكل مشــابه لتثبيت أي تطبيق آخر. وقد تتلقى تنبيهاً من «التحكم في قبول المســتخدم» (User Acceptance Control). اســمح لعملية التثبيت بالاستمرار بالنقر على زر «التالي».

٥. وقد تتلقى تحذيراً بأنه ســيتم إعادة تشــغيل اتصال الشبكة. إذا كانت هناك أنشطة على الشــبكة (كتحميل الملفات، أو الموســيقى، وما إلى ذلك) عليك الانتهاء من هذه الأنشطة كاملة قبل عملية المتابعة.

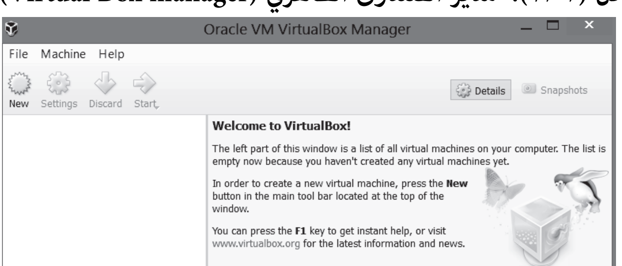
٦. وإذا طُلب منك تثبيت دعم الناقل التسلسلي العالمي (USB) من المُستحسن أن تختار تثبيت هذا الدعم.

٧. انقر على «إنهاء» لإكمال التثبيت. وعند اكتمال التثبيت، ستظهر رسالة تأكيد (الشكل ٢-١١). وإذا تم تمكين خانة الاختيار لبدء تطبيق الـ (VirtualBox) سيظهر لك مدير الصندوق الظاهري (Virtual Box manager) في الشــكل (٢-١٢)، وهو فارغ حالياً لكنك ســتقوم بملئه مع نظام تشــغيل لينكس الخاص بك في الخطوة الثانية من هذا التدريب العملي.

الشكل (٢-١١): تأكيد تثبيت الـ(VirtualBox)



الشكل (٢-١٢): مدير الصندوق الظاهري (Virtual Box manager)



الخطوة الثانية - تثبيت نظام التشغيل:

وكــما هو موضح في دليل إرشــادات الــ (VirtualBox) فإنه يُمكنــك تثبيت أي نظام تشــغيل حديث بوصفه نظام تشــغيل فرعي. وفي هذا الكتاب قمنا بتخصيص توزيع نظام التشــغيل لينكس، والذي يســمح لنا بالتحايل على قيود الترخيص التجارية. ولحسن الحظ فإن معظم المفاهيم الأمنية يمكِن تعميمها لأنظمة التشغيل، ومعظم المفاهيم الأمنية التي ســوف تتعلمها هنا تنطبق أيضاً على نظام تشغيل ويندوز. اتبع التعليمات التالية لتثبيت توزيع نظام التشغيل لينكس المُخصص في الآلة الافتراضية الجديدة في جهازك:

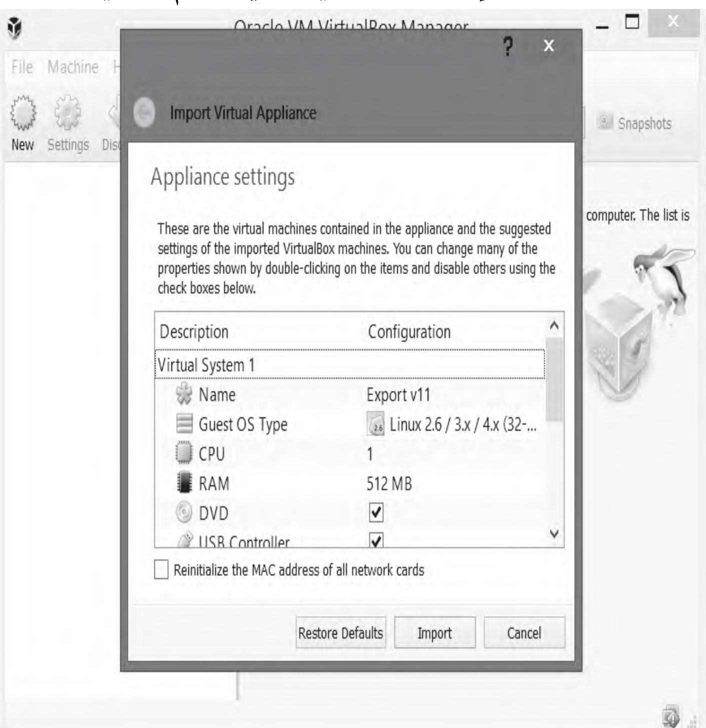
١.قــم بتحميل الصــورة الافتراضية لـ (CentOS Linux) من الموقــع الإلكتروني المرفق في الكتــاب. والمقصود بامتداد الملف (.ova) هو الجهــاز الافتراضي المفتوح (Open Virtual Appliance) وهــو معيــار صناعي لتثبيت حُزم أنظمة التشــغيل في الآلة الافتراضيــة[٢٧]. وهذا التصميم تم إنشــاؤه من قِبل شركــة (VMWare) وهي شركة رائــدة في الصناعــة الافتراضية. ولاحظ أن هذا الَملف كبير جــداً (أكبر من ٢,٥ جيجا بايت) ويمكن أن يســتغرق تحميله عدة ســاعات حتى وإن كنت تســتخدم الإنترنت ذات النطاق الواسع (Broadband).

٢.انقــر نقــراً مزدوجاً على ملــف CentOS_6.ova، وعندها ســيبدأ «معالج اســتيراد الأجهزة». وبالإمكان استخدام الإعدادات الافتراضية، كما يمكن البدء بإعداد في عملية إنشــاء الآلية الافتراضية عن طريق النقر على اســتيراد كما هو موضح في الشكل (٢-١٣). وقد تســتغرق عملية الاســتيراد من ١٠ إلى ٢٠ دقيقة بناءً على سرعة الكمبيوتر وموقع التثبيت.

---

(٢٧) لمعلومات أكثر انظر الموقع الإلكتروني التالي: http://fileinfo.com/extension/ova

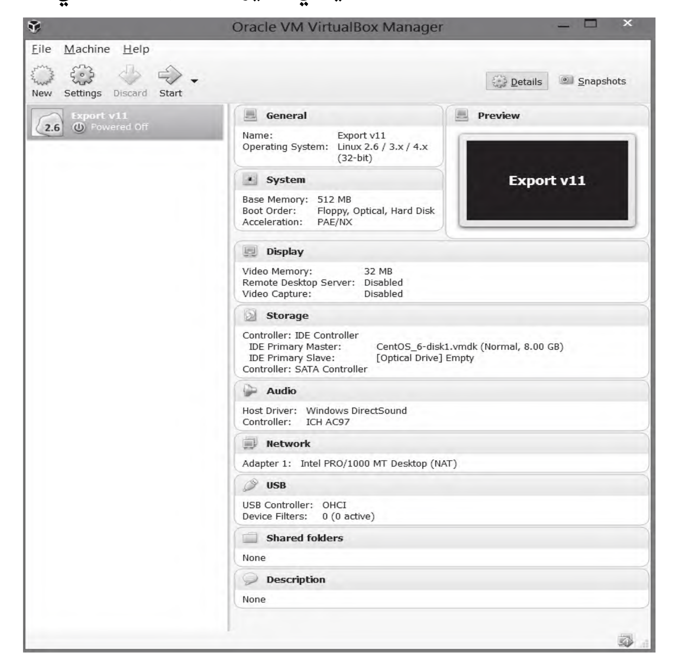
الشكل (٢-١٣): الإعدادات الافتراضية لاستيراد نظام التشغيل



٣.وعنـــد اكتـــمال التثبيت فإن مدير الصنـــدوق الافـــتراضي (Virtual Box manager) ســـيُظهر الآلة الافتراضية الجديدة في قائمة الآلات الافتراضية كما هو موضح في الشكل (٢-١٤). ومن الآن يمكنك تشغيل تطبيق الـ (VirtualBox)، واختيار الآلة الافتراضية والنقر على زر ابدأ لتشغيل الآلة الافتراضية. وبإمكانك النقر على زر «توقف» لإنهاء عمل الآلة الافتراضية.

٤.وفي هذه المرحلة قد تكون متحمســاً لمعرفة ما يؤدي إليه كل هذا. يمكنك الآن النقر على زر ابدأ بعد أن انتهيت من استيراد الآلة الافتراضية، وعندها سيبدأ نظام تشغيل لينكس. المشـــكلات الشـــائعة وحلولها موجـــودة أدناه. وبعد حل هذه المشـــكلات ستظهر لك شاشة (CentOS Linux) لتسجيل الدخول.

الشكل (٢-١٤): الآلة الافتراضية في مدير الصندوق الافتراضي



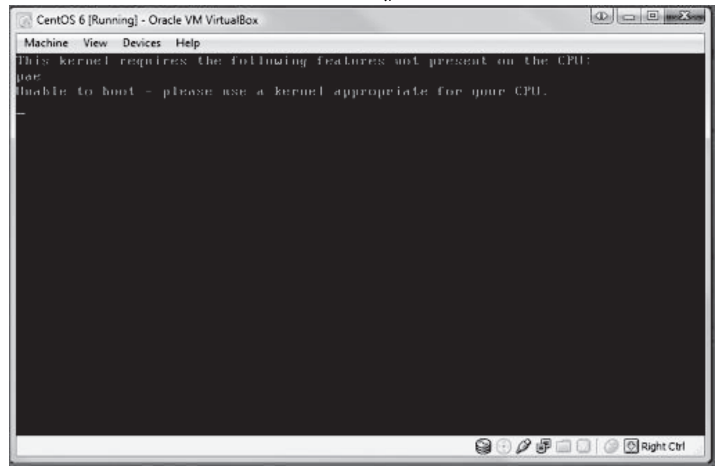
المشكلات المُحتمل حدوثها:

١. قــد تتلقى تحذيراً يشــير إلى أنك قمت بتحميل وتثبيت حزمــة كاملة وذلك لأن الـ (USB 2.0) مُفعــل في جهــازك. يمكنــك تجاهل هذا التحذير كــما يمكنك تحميل وتثبيت الحزمة الكاملة الموجودة في الموقع الإلكتروني لـ (VirtualBox).

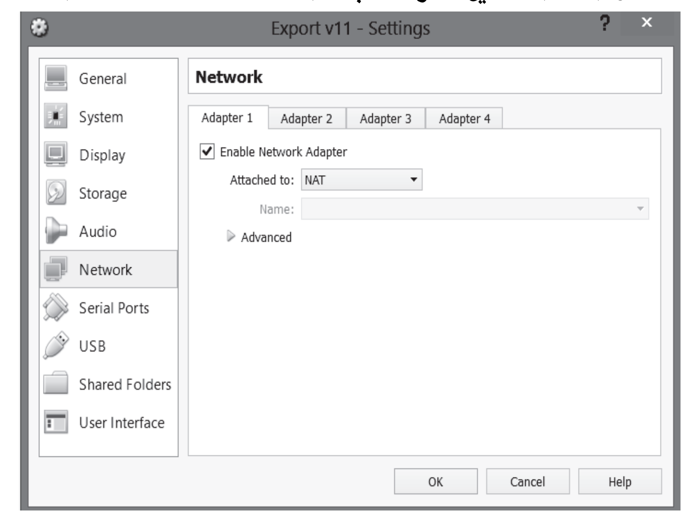
٢. وقد تتلقى رسائل تحذيرية بخصوص حركة الفأرة وحجم الإطار وما إلى ذلك. يمكنك أيضاً تجاهل هذه الرسائل.

٣. وقد تتلقى رســالة تفيد بوجود مشــكلة في وحدة المعالجة المركزية (CPU)، يُرجى اختيــار الآلة الافتراضية (VM)، ثــم الضبط (Settings) في مديــر الآلة الافتراضية (VM manager)، ثــم النظــام (System)، ثم المعالــج (Processor)، وبعد ذلك اختيار تمكين محول الشــبكة (enable PAE checkbox)، كما هو موضح في الشكل (٢-١٥) والشكل (٢-١٦).


الشكل (٢-١٥): خطأ في وحدة المعالجة المركزية

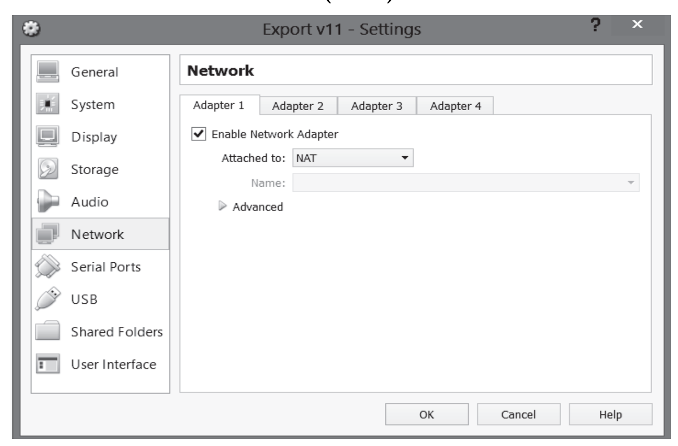


الشكل (٢-١٦): تمكين محول الشبكة (enable PAE checkbox)



٤. وإذا كنت غير قادر على الاتصال بالشبكة، انقر على إعدادات (Settings)، ثم شبكة (Network)، وقم بإرفاق محول الشبكة ١ (Network Adapter 1) إلى ترجمة عناوين الشبكة (NAT) كما هو موضح في الشكل (٢-١٧). كما يُمكنك النزول إلى الجزء السفلي من الصفحة الأولى ومن ثم اختيار الشبكة (Network).

الشكل (٢-١٧): إرفاق محول الشبكة ١ (Network Adapter 1) إلى ترجمة عناوين الشبكة (NAT)

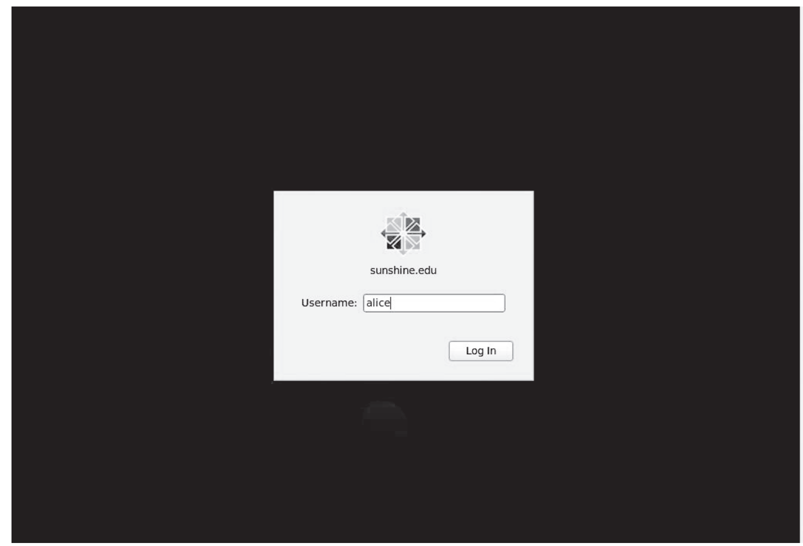


تشغيل الآلة الافتراضية:

١. عندما تبدأ الآلة الافتراضية بالعمل ســوف تشاهد شاشة الدخول كما هو موضح في الشكل (٢-١٨).



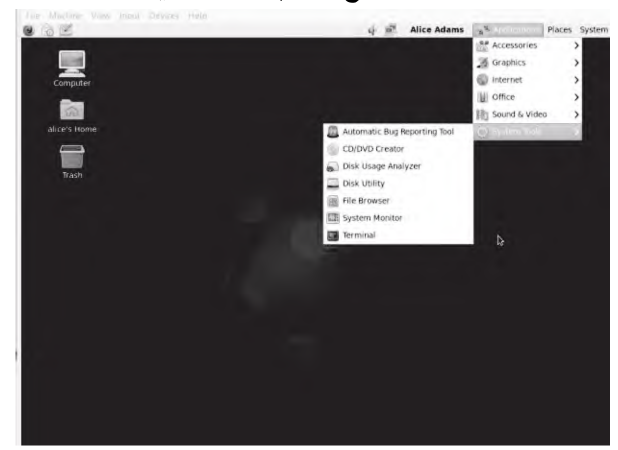
الشكل (٢-١٨): شاشة الدخول للآلة الافتراضية سينتوس



٢. أدخل اســم الدخــول (alice)، وكلمة المرور (.aisforapple)، بعد ذلك ســيظهر لك سطح المكتب الخاص بـ سينتوس كما في الشكل (٢-١٩)



الشكل (٢-١٩): سطح المكتب لسنتوس لينكس



أ- ولإيقاف الآلة الافتراضية اتبع ما يلي:

- في أجهزة الويندوز: (Machine) ← إغلاق (Close)
- في أجهزة الماك: (Virtual Box) ← إنهاء (Quit)

ب- ولتشغيل الآلة الافتراضية مرة أخرى اتبع ما يلي:

- في أجهــزة الويندوز: ابدأ (Start) ← البرامــج (Oracle) ← Programs) (Oracle VM VirtualBox ← (VM VirtualBox)
- في أجهزة الماك: (Virtual Box) ← (Applications)

٣. في الفصل القادم ســوف تتعلم بعض الأساسيات عن: إدارة أنظمة ينكس/لينكس بما في ذلك التنقل في المجلدات، واستخدام المحرر السادس (vi editor)، وإنشاء حسابات المستخدمين.

أسئلة على نشاط التدريب العملي:

١. اشرح بشكل مختصر تطبيق الـ (VirtualBox) وأهم استخداماته.

٢. اشرح بشكل مختصر تنسيق الملف OVA.

لتوضيح أنك قمت بتثبيت الآلة الافتراضية بنجاح قم بما يلي:

١. خُذ صورة من الشاشة لسطح المكتب الخاص بـ سينتوس (CentOS).

٢. قم بتشغيل متصفح الإنترنت من خلال: تطبيقات (Applications)← الإنترنت (Internet)← متصفح الفايرفكس (Firefox)، ثم قم بأخذ صورة من الشاشة لنافذة المتصفح تعرض الصفحة الرئيسية الافتراضية للمتصفح.

٣. قم بتشغيل مراقب النظام من خلال: تطبيقات (Applications)← أدوات النظام (System tools) ← مراقب النظام (System monitor) ثم قم بأخذ صورة من شاشة لمراقب النظام.

٤. قم بتشغيل الوحدة الطرفية من خلال: تطبيقات (Applications)← أدوات النظام (System tools) ← الوحدة الطرفية (Terminal)، وفي صفحة موجه الأوامر أدخل الأمر (whoami)، ثم قم بأخذ صورة من الشاشة لنافذة الوحدة الطرفية توضح الأمر ومُخرجاته (سنستخدم نافذة الوحدة الطرفية بشكل كبير في مُعظم أنشطة التدريب العملي في هذا الكتاب).

٥. قم بإيقاف الآلة الافتراضية من خلال: الآلة (Machine) ← إغلاق (Close) ← إطفاء الآلة (Poweroff the machine).

تمرين التفكير النقدي - الحكم بالسجن على مديرين تنفيذين في شركة جوجل بسبب فيديو:

في شهر سبتمبر من عام ٢٠٠٦ قام أربعة من الزملاء بالتنَمُّر على صبي يعاني من مرض التوحد وذلك في مدرسة في مدينة تورين بإيطاليا. وقاموا بتصوير ذلك في مقطع الفيديو، كما قاموا بنشره على موقع اليوتيوب التابع لشركة جوجل. انتشر مقطع الفيديو وأصبح مشهوراً حيث تمت مشاهدته أكثر من ٥,٥٠٠ مرة خلال شهرين. كما وصل هذا المقطع إلى قائمة «الفيديو الأكثر تسلية» في موقع جوجل الإيطالي.

وعندمـا تم إعلام شركة جوجل بذلك مـن قِبل الشرطة الإيطالية قامـت بإزالة مقطع الفيديـو. لكن والد الطفل ومنظمة فيفـي داون (Vivi Down)، وهي المنظمة التي تُمثل الأشـخاص المصابين بمتلازمة داون، رفعوا دعوى قضائية ضد أربعة من المديرين التنفيذين في جوجل بتهمة التشهير ومعالجة البيانات الشخصية بصورة غير مشروعة. وادعت جوجل أنها تجاوبت بشكل سريع بإزالة مقطع الفيديو عندما تم إبلاغها.

وفي الرابع والعشرين من شهر فبراير من عام ٢٠١٠ بَرّأت محكمة ميلانو جميع المديرين التنفيذين من تهمة التشـهير، لكن المحكمة رأت أنّ ثلاثة من المديرين التنفيذين مذنبون في معالجة البيانات الشخصية بصورة غير مشروعة، وفي تباطئهم في إزالة الفيديو عندما تم إبلاغهـم من قبل الشرطة. وهؤلاء المديرون هم: نائب الرئيس ومدير الشـؤون القانونية ديفيـد دروموند، والعضو السـابق بمجلس إدارة جوجل الايطالي جـورج دي لوس رييس، ومستشـار الخصوصية العالمية بيتر فليشر. وتم تحميلهم المسـؤولية الشخصية بذلك لأن القانون الإيطالي ينص على أن الموظفين مسؤولون قانونياً عن أنشطة الشركات التي يعملون فيهـا. ولم يكن هؤلاء المديـرون في إيطاليا وقت المحاكمة، كما تـم تعليق الحكم بانتظار الاستئناف لذا لم يكن أي منهم تحت التهديد المباشر بالسجن.

وكان موقـف جوجل الذي عبر عنـه مدير اتصالاتها بأنهـم «لم يقوموا بتحميل مقطع الفيديـو، ولم يقوموا بتصويره، ولم يقوموا بمراجعته، ومع ذلك فقد تم الحكم عليهم بأنهم مذنبـون». وفي حكـم القاضي الذي احتوى على ١١١ صفحة كتب القاضي أوسـكار ماجي «الإنترنت ليسـت البراري اللامحدودة التي يُسـمح فيها بكل شيء ولا يُمنع منها شيء...بدلاً من ذلك هناك قوانين تنظم السلوك وإذا لم تُحترم القوانين فإن العواقب الجزائية قد تترتب عـلى ذلـك». وتبعاً للقانـون الإيطالي فإن عدم إيقـاف حقيقة ما، يُعادل ما يُسـبب تلك الحقيقـة. لذا يتطلـب قانون حماية البيانات الحصول على إذن مسـبق قبل التعامل مع البيانات الشخصية. لكن شريط الفيديو المنشور احتوى على بيانات شخصية. ولذلك كانت جوجل مسـؤولة عن التأكد من أن المستخدم الذي نشر الفيديو حصل على موافقة كل من شـارك في الفيديو. وفي الحادي والعشرين من شـهر ديسمبر من عام ٢٠١٢ ألغت محكمة الاستئناف الإيطالية الإدانة وبرأت المديرين التنفيذيين.

المراجع:

Manuela D' Alessandro, "Google executives convicted for Italy autism video," 02/24/2010, http://www.reuters.com/article/201024/02//us-italy-google-conviction-idUSTRE61N2G520100224 (accessed 07/16/2013).

Hooper, J. "Google executives convicted in Italy over abuse video," The Guardian, 02/24/2010, http://www.guardian.co.uk/technology/2010/feb/24/google-video-italy-privacy-convictions (accessed 07/16/2013)

Povoledo, E. "Italian judge cites profit as justifying a Google conviction," New York Times, April 12, 2010.

EDRi-gram, "First decision in the Italian criminal case against Google executives," 02/24/2010, http://www.edri.org/edrigram/number8.4/decision-italy-vs-google-executives (accessed 07/16/2013).

Pfanner, E. "Italian appeals court acquits 3 Google executives in privacy case," New York Times, December 21, 2012.

أسئلة على تمرين التفكير النقدي:

١. ما رأيك في تلك الحادثة؟

٢. هل يُفترض أن يكون مسؤولو الأنظمة والشركات مسؤولين عن محتوى ما ينشره المستخدمون في الموقع الإلكتروني التابع للشركات؟

٣. افترض أنك مسؤول النظام لموقع ما، وأنك تلقيت طلباً من أحد المُستخدمين بحذف صورة تم تحميلها بواسطة صديق في حفلة كان المستخدم حاضراً فيها. هل تعتقد أن هذا الطلب معقول؟

٤. كيف ستستجيب لطلب كهذا؟

تصميم حالة:

لتصميم هذه الحالة سنعتمد على جامعة ولاية الشمس المشرقة التي تعرضنا لها في الفصل الأول. وبشكل مشابه للعديد من الخدمات الأخرى المتعلقة بتقنية المعلومات في الجامعة، ينقسم دعم البريد الإلكتروني إلى نظامين رئيسيين هما:

١. تقوم إدارة تقنية المعلومات، والتي ترجع إلى نائب الرئيس لشـؤون المال والأعمال، بدعـم البريد الإلكتروني لجميع الموظفين الإداريين. ولأسـباب تاريخية، يقوم مكتب المدير (نائب الرئيس للشؤون الأكاديمية) بالدفع لإدارة تقنية المعلومات لدعم البريد الإلكتروني لأعضاء هيئة التدريس أيضاً.

٢. البريد الإلكتروني الخـاص بالطلاب يتم دعمه من خلال موظفي الدعم الفني الذين يرجعون إلى عميد شؤون الطلاب.

ويعمل نظام البريد الإلكتروني للطلاب على خادم واحد تم شراؤه قبل ست سنوات. ويحتوي الخـادم على اثنين من محركات الأقراص الداخلية. وتحتـوي محركات الأقراص الداخلية على نظام التشغيل والتطبيقات ومجموعة من الأقراص الخارجية (JBOD) التي تحتوي على جميع البيانات. كما يحتوي الخادم على مصدر واحد للتيار الكهربائي ومنفذ شـبكة واحد. ويعمل الخادم على نظام لينكس (Linux) وعلى برنامج (Sendmail) لتسـليم البريد الإلكتروني وهو برنامج مفتوح المصدر ويعتمد على بروتوكول إرسال البريد البسيط (SMTP).

وتسـببت إحدى المشكلات الأخيرة في القرص الداخلي إلى تحطم خادم البريد الإلكتروني للطـلاب. عنـد حدوث ذلـك للمرة الأولى كان هنـاك انقطاع في الخدمة لمدة ١٣ سـاعة. وللأسف لم يتم معرفة سبب انقطاع الخدمة مما أدى إلى حدوث المشكلة مرة أخرى، لكنها كانت أكثر خطورة، إذ فُقد جميع رسـائل البريد الإلكتروني بسـبب مشكلة خطيرة في حفظ الرسـائل. ولم يتمكن المسـؤول عن النظام والقائم بأعمال الخادم من التعامل مع ضغوط العمل وقدم اسـتقالته. وعلى فرض أنك كنت المُسـاعد لمسؤول النظام وكان عميد شؤون الطلاب في مأزق وعرض عليك وظيفة براتب كبير وبدلات كما وفر لك برنامجاً لإعفائك من رسوم الدراسة لمساعدتك في التخرج من الجامعة[٢٨].

وبعد الحادثة بأسبوعين عاد الخادم إلى العمل وتم استعادة جميع رسائل البريد الإلكتروني من الشريط. وبما أن المشكلة حدثت الساعة الواحدة بعد الظهر، والنسخ الاحتياطي الأخير تم في الساعة الثانية صباحاً من يوم الثلاثاء، فإنه لا يمكن استعادة البريد الإلكتروني الذي تم تسليمه بين هذين الوقتين وتم فقده نهائياً.

(٢٨) على الرغم من أن هناك بعض الدراما فيما ذُكر، إلا أن هذا السيناريو يعتمد على حادثة حقيقية.

وكان الطـلاب غاضبين جداً مما أدى إلى تدخل مديــر الجامعة. وطُلب منك مع عميد شؤون الطلبة أن تقدم توصية لأحد الخيارات التالية مع توضيح أسباب التوصية:

- صيانة خوادم البريد الإلكتروني محلياً.
- اســتبدال كامل البنية التحتية للبريــد الإلكتروني بـ (البرمجيات كخدمة) (Software as a Service).
- اســتخدام تطبيقات جوجل للتعليــم (GoogleApps for Education) https://www.google.com/apps/intl/en/edu/

أسئلة على تصميم الحالة الأمنية:

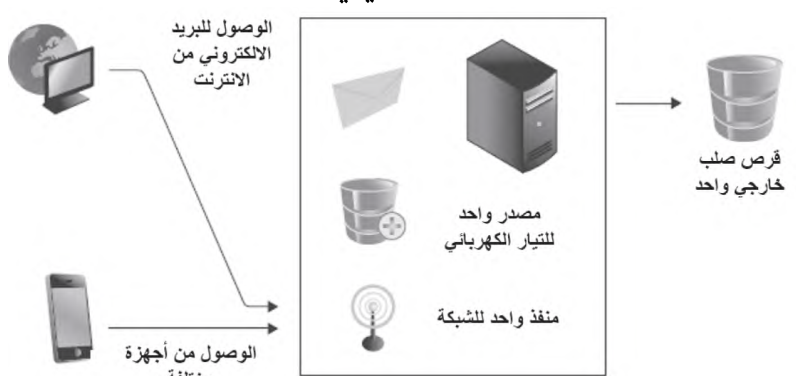
١. ما هي مجموعة الأقراص الخارجية (JBOD)؟

٢. في خطوة لدراسة الخيارات السابقة لجامعة ولاية الشمس المشرقة ننصح بإجراء عام وهو النظر فيما يقوم به زملاؤك الآخرون وهو ما يُســمى في إدارة الأعمال بالمقارنة المرجعية. وفي الســياق الخاص بك تنصح أن تنظر فيما تقوم به الجامعات المناظرة لجامعتك بخصوص إدارة أنظمة البريد الإلكتروني.

- (أ) اذكــر ثلاث جامعــات أو كليات في منطقتك تعتقد أنهــا تمثل نظائر قريبة لجامعة ولاية الشمس المشرقة (اجعل هذه القائمة في متناول يدك لأنك ستجد نفســك ترجع إلى هذه القائمة باســتمرار لدراســة ما تقوم به هذه الجامعات لمواجهة التحديات التي تواجهها في هذا الفصل والفصول اللاحقة).
- (ب) أيّ مــن الخيارات الســابقة المتعلقة بإدارة البريــد الإلكتروني موجودة في الجامعــات التي حددتها؟ لمــاذا اختارت الجامعات هــذه الخيار؟ (بإمكانك العثور عــلى معلومات حول هذا الموضوع في موقعهــم الإلكتروني، كما يمكنك الاتصال هاتفياً بالدعم الفني).
- (ج) إذا لم تكن جامعتك مذكورة في القائمة التي حددتها في (أ)، ما الذي تقوم به جامعتك لإدارة خدمات البريد الإلكتروني؟ ولماذا؟

٣. ما المشــكلات التي تتوقع حدوثها في النظام الحالي لجامعة ولاية الشــمس المشرقة الموضح في الشــكل (٢-٢٠)؟ ما نقاط العطل المفردة (single points of failure)؟ ومــا الذي يجب عمله للنظام المحلي حتى يتمكن التعامل بأمان مع خدمات البريد الإلكتروني في حال تعطل أي نقطة من نقاط العطل المفردة؟

الشكل (٢-٢٠): البنية التحتية للبريد الإلكتروني في جامعة ولاية الشمس المشرقة



٤. ما المميزات (إن وجدت) التي تســتطيع الحوســبة الســحابية (البرمجيات كخدمة (Software as a Service)، والبنيــة التحتيــة كخدمــة (Infrastructure as a Service) تقديمها والتي لا يمكن توفريها محلياً؟

٥. خلال دراســتك للخيارات السابقة وجدت أن أحد الاستفسارات الشائعة لدى الدعم الفني يتعلق بـ (استعادة البريد الإلكتروني المحذوف من غير قصد). ما الوسائل (إن وجدت) التي توفرها الخيارات السابقة لاستعادة البريد الإلكتروني المحذوف من غير قصد؟

٦. يطلب معظم الطلاب ميزة مهمة أخرى وهي الوصول إلى البريد الإلكتروني من الأجهزة المختلفة كالهواتف الذكية، وكذلك الوصول إلى البريد الإلكتروني من تطبيقات البريد الإلكتروني التقليدية كـ (Thunderbird) و (Eudora). ما الدعم الذي يقدمه كل خيار من الخيارات السابقة للوصول إلى البريد الإلكتروني من الأجهزة المختلفة؟ وما مزايا وعيوب كل خيار لتحقيق هذا الوصول؟

الفصل الثالث

إدارة النظام (الجزء الثاني)

نظرة عامة:

في الفصل الســابق ناقشــنا موضوع إدارة النظــام وقدمنا وصفاً للــدور الذي يقوم به مســؤولو النُظم في أمن المعلومات. وفي هذا الفصل سنســتمر بمناقشــة إدارة الأنظمة من خلال تقديم مجموعة أساســية من العمليات التقنية المســتخدمة من قبل مسؤولي النُظم. وســيتم تطبيق هذه العمليات التقنية باستخدام آلة لينكس الافتراضية التي جرى إنشاؤها في الفصل السابق. وفي نهاية هذا الفصل يجب أن تعرف:

- المكونات الأساسية لأنظمة التشغيل الحديثة.
- كيفية استخدام واجهة سطر الأوامر (command-line interface).
- العمليات الأساسية للتنقل في نظام الملفات.
- أذونات الملفات للمستخدمين والمجموعات.
- إدارة حساب المستخدم.
- إدارة البرمجيات.

هيكلة نظام التشغيل:

أنظمة تشغيل الحاســب الآلي هي برمجيات تدير مكونات أجهزة الحاسب الآلي وتوفر الخدمات العامة لتطبيقات المســتخدم. وتتكون أنظمة التشــغيل الحديثة من العديد من البرمجيات (أو العمليات) المنفصلة التي تعمل معاً لتحقيق النتائج المطلوبة (الشكل ٣-١). مركزيــاً تمثل نواة نظــام التشــغيل (kernel) البرنامج الذي يتحكــم في مكونات الأجهزة، وإدارة الذاكــرة، وتنفيذ التعليمات البرمجية على وحدة المعالجة المركزية، وإخفاء التفاصيل الضمنية لقطع الأجهزة من تطبيقات المســتخدم. ويســمح ذلك لمطوري البرامج بتجاهل

التفاصيل الضمنية لقطع الأجهزة عند تطوير التطبيقات مما يُسهم بشكل كبير في تبسيط تطوير التطبيقات.

أما القشرة (shell) فهي برنامج نصي يسمح للمستخدم بالتفاعل مباشرة مع نواة نظام التشغيل (kernel). وتشمل العمليات العامة التي تقوم بها القشرة: تشغيل وإيقاف البرامج، والتحكم في تنفيذ البرامج، وبدء وإيقاف جهاز الحاسب الآلي. كما تقوم القشرة بإخفاء تعقيد نواة نظام التشغيل (kernel) عن المستخدم، بحيث يستطيع المستخدم إدخال الأوامر بلغة إنجليزية واضحة ومن ثم الاعتماد على القشرة (shell) لترجمة هذه الأوامر إلى الرمز الثنائي حتى تقوم نواة نظام التشغيل (kernel) بتنفيذها.

الشكل (٣-١): هيكلة نظام التشغيل

User Applications	تطبيقات المُستخدم
Shell	القشرة
Kernel	نواة نظام التشغيل
Device Drivers	برامج تشغيل الجهاز
Hardware	قطع الجهاز

وبينما تقوم أنظمة التشغيل الرسومية، كنظام تشغيل ويندوز، بإخفاء القشرة (shell) فإن أنظمة التشغيل المُعتمِدة على ينكس (Unix)، مثل لينكس (Linux) وماك أو إس إكس (Mac OSX)، تقوم بتشغيل القشرة (shell) تلقائياً عند بدء التشغيل. وهذه القشرة تعمل من خلف الستار بحيث تقوم ببدء وإيقاف البرامج استجابة لعمليات واجهة المستخدم الرسومية (GUI). ويمكن أيضاً الوصول مباشرة إلى هذه القشرة بوصفها وحدة طرفية (terminal)، وهذه الوحدة الطرفية هي البيئة المفضلة والمُستخدمة من قبل مسؤولي النُظم عند أداء مُعظم مهام إدارة النظام. وفي هذا الكتاب سيتم تنفيذ جميع مهام إدارة النظام باستخدام إطار الوحدة الطرفية في نظام التشغيل لينكس ما لم يتم النص على خلاف ذلك.

الجدول (٣-١): برامج القشرة الشائعة

الاسم	المطور	تاريخ الإصدار الأول	التفاصيل
قشرة بورن Bourne) (Shell	ستيفن بورن	١٩٧٧	المعيار الواقعي في ينكس حيث إن كل نظام تشغيل مُعتمد على ينكس لا يخلو من قشرة واحدة على الأقل متوافقة مع قشرة بورن[1].
قشرة سي (C (Shell	بيل جوي	١٩٧٨	تعتمد صياغة الأوامر على إحدى لغات البرمجة وهي لغة السي. هذه القشرة منتشرة في الاستخدام التفاعلي لكن لا يُنصح باستخدامها كلغة برمجة نصية[1].
قشرة كورن (Korn Shell)	ديفيد كورن	١٩٨٣	متوافقة مع معيار الواجهة البينية لنظام التشغيل القابل للحمل لنظام التشغيل اليونيكس (posix) رقم ١٠٠٣,٢، ومتوافقة أيضاً مع قشرة بورن، كما تُضيف العديد من الميزات اللازمة للبرمجة النصية[٣].
قشرة باش Bourne-) again (Shell-Bash	براين فوكس	١٩٨٩	صُممت لتكون بديلاً مفتوح المصدر لقشرة بورن. قشرة باش شائعة الاستخدام في البرمجة النصية والاستخدام التفاعلي لأنها تجمع بين العديد من ميزات قشرة سي وقشرة كورن، كما تُضيف العديد من التحسينات الخاصة بها[٤].

ومثـل بقية البرمجيـات فإن القشرة (shell) تطورت مع مـرور الزمن. ويُقدم الجدول (٣-١) لمحة عامة عن أنواع القشرة المُتاحة. وأكثر مسؤولي النُظم يفضل قشرة باش (Bash shell) وهي القشرة المستخدمة في هذا الكتاب.

(1) https://en.wikipedia.org/wiki/Unix_shell

(٢) http://www.faqs.org/faqs/unix-faq/shell/csh-whynot/

(3) Rosenblatt, B. Learning the Korn Shell. (O'Reilly), 1993

(4) http://www.gnu.org/software/bash/manual/bashref.html#What-is-Bash_003f

تشغيل القشرة في نظام الويندوز

هناك العديد من الخيارات لتشغيل القشرة على نظام مايكروسوفت ويندوز. ولم تتغير أوامر القشرة الرئيسية كثيراً في نظام الميكروسوفت منذ منتصف التسعينيات حيث يتم استخدام (COMMAND.COM) أو (cmd.exe) بناءً على إصدار ويندوز. وتقوم القشرة بتنفيذ الأوامر ودعم عدد قليل من الأدوات الأساسية لمعالجة نظام الملفات. وعلى الرغم من أن الإصدارات اللاحقة قد أضافت إمكانية الاتصال بالشبكة المحلية لنقل الملفات والإدارة عن بعد، إلا أن قدرات القشرة بشكل عام تظل محدودة.

يتضمن النظام الحديث من مايكروسوفت قشرة ولغة برمجة نصية بديلة تدعى ويندوز بورشل (Windows Powershell)[٥]. وتم تصميم بورشل في المقام الأول للبرمجة النصية، وتتميز نسبياً عن بقية أنواع القشرة بأنها لغة موجهة بالكائنات (object-oriented language) يمكنها التفاعل مباشرة مع مكونات وتطبقات (.NET). وأصبحت بورشل بشكل سريع لغة البرمجة النصية في ويندوز، كما أن العديد من التطبيقات الرئيسية الأخرى، مثل (Microsoft Exchange ٢٠١٠)، تعتمد عليها بشكل كبير[٦].

وبالإضافة إلى القشرة التي صممتها مايكروسوفت، فإن مطوري برمجيات المصادر المفتوحة قاموا بإعادة تكوين الكثير من بيئة نظام ينكس لتعمل في نظام ويندوز بما في ذلك الأنواع الشائعة لقشرة ينكس. وفي التسعينيات قد تم تطوير مشروع سيغوين (Cygwin project)، وذلك للسماح للبرامج التي تعمل على نظام ينكس أن تعمل أيضاً على نظام ويندوز. وقد تطور المشروع إلى مجموعة من البرمجيات التي توفر بيئة مشابهة تماماً لبيئة ينكس بما في ذلك أوامر القشرة والبرامج الرسومية. وتُعد قشرة باش هي القشرة الافتراضية في مشروع سيغوين (Cygwin project)، لكن عملياً جميع الأنواع الشائعة للقشرة والمُستخدمة في توزيع لينكس متوفرة من خلال مُثبت سيغوين.

واجهة سطر الأوامر (command-line interface):

قبل الشروع في مهام إدارة النظام نستعرض في هذا القسم واجهة سطر الأوامر وأساسيات استخدام هذه الواجهة (الشكل ٣-٢).

(5) http://technet.microsoft.com/en-us/library/bb978526.aspx

(6) http://social.technet.microsoft.com/wiki/contents/articles/exchange-2010-powershell-scripting-resources.aspx

موجه باش (The Bash prompt):

لتشــغيل الوحدة الطرفية في إصدار ســينتوس لينكــس (CentOS Linux) المتوفر مع هــذا الكتاب، افتح لوحة أدوات النظام (System Tools) الموجودة تحت قائمة التطبيقات (Applications) كما هو موضح في الشكل (٣-٢). وعند فتح نافذة الوحدة الطرفية سترى موجــه من قشرة باش. ويعــد موجه باش نقطة الدخول لجميــع الأوامر التي تكتبها، كما يمكن أن يقدم موجه باش معلومات حول الحســاب والخادم الذي تســتخدمه والبيئة التي يعمل فيها باش. وهذا مثال تقليدي على موجه باش:

```
[alice@sunshine usr]$
```

الملفات والأدلة:

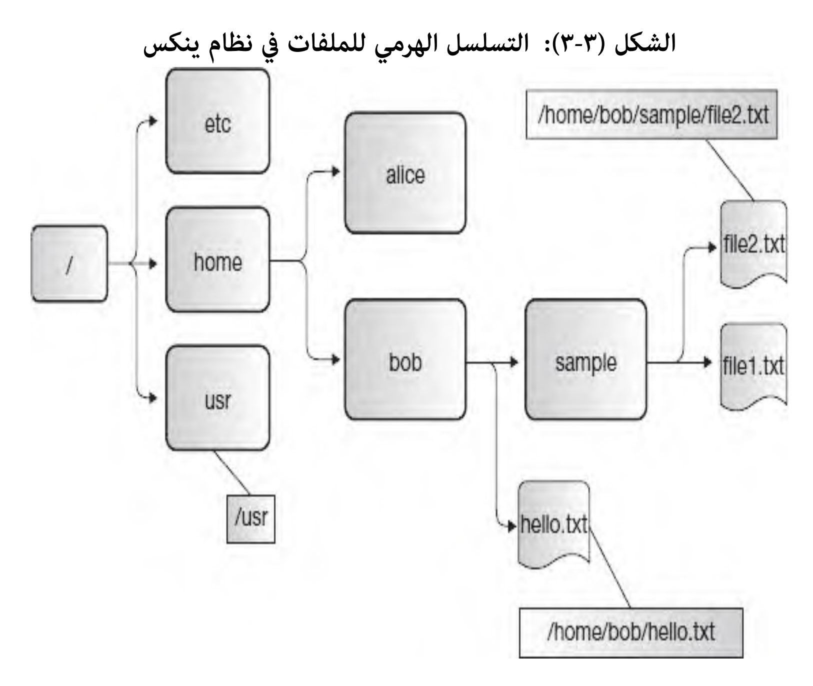
يتــم تنظيم الملفــات والأدلة في جميع أنظمة التشــغيل في هيكلة هرميــة. وفي نظام يونيكس يتم فصل كل «طبقة» من التسلسل الهرمي بخط مائل (/). ويُشار إلى قمة الهرم بـــ «جذر نظام الملفات» ويتم تمثيلها بخــط مائل واحد. ومن الممكن أن يحتوي كل دليل على ملفات أو أدلة فرعية أو مزيج من الاثنين معاً (الشكل ٣-٣).

وفي التسلسل الهرمي يُشــار إلى مكان الملف أو الدليل بمساره، وهناك طريقتان للتعبير عن مسار الملف كما هو موضح في الجدول (٣-٢).

الشكل (٣-٢): الوصول إلى نافذة موجه الأوامر



الشكل (٣-٣): التسلسل الهرمي للملفات في نظام ينكس



الجدول (٣-٢): تحديد مسار الملف

النوع	أمثلة	الوصف
مسار مطلق	home/bob/hello.txt/etc/	المسار المطلق هو المكان المحدد للملف الذي تتم الإشارة إليه. ويشمل كل دليل فوق الدليل الحالي حتى الوصول إلى جذر نظام الملفات.
مسار نسبي	sample/file2.txt hello.txt	المسار النسبي يحدد مكان الملف بالنسبة إلى الدليل الحالي.

الحساسية لحالة الأحرف

يمكــن القول إن جميع ملفات ينكس هي ملفات حساســة لحالة الأحــرف فملف (hello.txt) يختلف عن ملف (HELLO.TXT). واســتثناءً لهذه القاعدة فإن نظام الملفات الافتراضي المستخدم في نظــام ماك أو إس إكس (HFS+) يُعد غير حســاس لحالة الأحــرف. ففي نظام ماك أو إس إكس (Mac OSX) ســيتم اعتبار ملــف (hello.txt) وملف (HELLO.TXT) على أنهما الملف نفســه. ولهذا السبب من الضروري التحقق من التعارض المُحتمل في أسماء الملفات، وذلك عند نسخ الملفات من نظام حساس لحالة الأحرف إلى نظام ملفات غير حساس لحالة الأحرف.

التنقل في نظام الملفات - الأوامر (pwd،cd):

أول شيء تحتــاج لمعرفته هو موقعك الحــالي في نظام الملفات، ويقوم أمر (pwd) بهذه المهمــة حيث يُمثل هذا الأمر طباعة الدليل الحــالي (print working directory)، ويقوم بإرجاع المســار المطلق للدليل الذي تتواجد فيه حالياً. وعند تســجيلك الدخول على نظام ينكس أو عند فتح نافذة وحدة طرفية، سيكون موقعك عادة في الدليل الرئيسي. وفي نظام ينكس يُعد الدليل الرئيسي مكانك الخاص وهو مشابه لمجلد المستندات في نظام ويندوز.

[alice@sunshine ~]$ pwd

/home/**alice**

وللانتقال إلى دليل آخر يمكنك استخدام أمر (cd) وهو الأمر الخاص بتغيير الدليل والذي يسمح بالتبديل إلى دليل آخر. ويتم تحديد اسم المجلد المستهدف كمعامل للأمر.

[alice@sunshine ~]$ **cd /usr**

[alice@sunshine usr]$ **pwd**

/usr

وهكذا فإن الأمر (cd /usr) قد أخذنا إلى مجلد (/usr). وفي هذه الحالة تم اســتخدام المسار المطلق للدليل. وبالإمكان أيضاً استخدام المسار النسبي.

```
[alice@sunshine usr]$ cd bin
[alice@sunshine bin]$ pwd
/usr/bin
```

ماذا عن الصعود إلى أعلى التسلسل الهرمي؟ وبعبارة أخرى كيف يتم الانتقال من (/usr/bin) إلى (/usr). بالإمكان استخدام طريقة المسار المطلق الموضحة أعلاه، ولكن هناك طريقة أخرى. الدليل الأم (Parent Directory) هو الدليل الذي يأتي مباشرة بعد الدليل الحالي في التسلسل الهرمي، ويتم تمثيله بنقطتين (..).

```
[alice@sunshine bin]$ pwd
/usr/bin
[alice@sunshine bin]$ cd ..
[alice@sunshine usr]$ pwd
/usr
```

وبالمثل فإن الدليل الحالي يتم تمثيله بنقطة واحدة (.)، وهذا لن يكون عملياً عند تغيير الأدلة لأن الأمر (cd) سيوجه القشرة لتغيير الأدلة إلى الدليل الحالي (أي بعبارة أخرى عدم فعل أي شيء)، لكنه سيكون مفيداً مع بعض الأوامر الأخرى التي سنتعلمها.

سَرد الملفات والأدلة:

لسَرد محتويات الدليل الحالي استخدم الأمر (ls).

```
[alice@sunshine usr]$ cd /home/alice
[alice@sunshine ~]$ ls
Desktop  Documents  Downloads  hello.txt Music Pictures Public
Templates  Videos
```

ووفقاً لإصدار وضبط نظام التشـغيل الذي تسـتخدمه قد تظهر النتائج في ألوان متعددة لتمثـل الأنواع المُختلفة من الملفات والأدلة المعروضة. (وفي هذه الحالة فإن العناصر باللون الأزرق تمثل الأدلة، وتلك التي باللون الأسود تمثل الملفات). ولأن هذه الألوان قد تختلف من إصدار نظام تشغيل إلى اصدار آخر فمن الأفضل عدم الاعتماد عليها. وهناك وضع بديل، أو مفتاح يمكن تمريره لأمر (ls) من أجل عرض النتائج في شكل موحد، وهذا المفتاح هو (F-)

```
[alice@sunshine ~]$ ls -F
Desktop/  Documents/  Downloads/ hello.txt Music/ Pictures/
Public/  Templates/  Videos/
```

ويقوم الأمر (ls -F) بإضافة خط مائل (/) لكل دليل. ويمكنك الآن التمييز بسهولة بين الملفـات والأدلة. لكن الأمـر (ls) لا يقوم افتراضياً بعرض الملفات المخفية في الدليل. وتُعد جميع الملفات و/أو الأدلة التي تبدأ أسـماؤها بنقطة (.) ملفات مخفية. والملفات المخفية هي الملفات التي يتم افتراضياً إخفاؤها عن المستخدمين. ولعرض جميع الملفات بما في ذلك الملفات المخفية يتوجب استخدام مفتاح (a).

```
[alice@sunshine  ~]$ ls -aF
./            .bash_logout   Desktop/    hello.txt  Public/
../           .bash_profile  Documents/  Music/     Templates/
.bash_history   .bashrc        Downloads/  Pictures/  Videos/
```

وكما ترى فإن العديد من الملفات المخفيـة (.bash_history, .bash_logout، وغيرها) أصبحت غـير مخفية الآن. وكذلك فإن اثنين من إدخالات الأدلة / (current directory)، و/ (parent directory) أصبحـت غير مخفية الآن. وبمـا أن جميع الأدلة في نظام ينكس تنتمي إلى إدخالات الدليل الحالي وتنتمي كذلك إلى دليل الأم سيكون هناك دائماً اثنين على الأقل من ادخالات الأدلة المخفية في كل دليل.

عند فحص النظام انتبه للملفات المخفية حيث يســتخدم المهاجمون خدعة شائعة وهي تمويه الدليــل الذي يحتــوي على أدوات الهجوم، وذلك بإعادة تســمية الدليل بثــلاث نقاط (...) وهذه طريقة فعالة للاختفاء عن الرؤية العادية. ومن الســهل جداً أن تنطلي عليك هذه الخدعة إلا إذا كنت منتبهاً لها.

```
[alice@sunshine compromised]$ ls -aF
./   .../     Documents/  hello.txt Pictures/ Templates/
../  Desktop/  Downloads/  Music/    Public/   Videos/
```

امتدادات القشرة:

الامتدادات هي رموز خاصة أو مقاطع تســتخدمها القشرة لبناء قائمة الملفات أو الأدلة، والتي تعمل على أساســها الأوامر. وهناك العديد من الأنواع المختلفة للامتدادات المعروفة في قشرة باش.

امتداد المدّة (Tilde):

والمقصود بامتداد المدّة (~) في قشرة باش هو الدليل الرئيسي للمستخدم

```
[alice@sunshine Expansion]$ cd ~
[alice@sunshine ~]$ pwd
/home/alice
```

وإذا وضعت اســم المســتخدم بعد المدّة فإن قشرة باش تُشير إلى موقع الدليل الرئيسي الخــاص بهذا المســتخدم. ولــن تتمكن من اســتخدام الأمر (cd) في الدليــل الرئيسي لهذا المســتخدم إلا إذا منحك هذا المســتخدم الإذن للقيام بذلك، وهذا مثال على استخدام هذا النوع من الامتداد.

```
[alice@sunshine Expansion]$ cd ~bob
```

```
[alice@sunshine ~]$ pwd
/home/bob
```

امتداد اسم الملف – رموز البدل (wildcards):

لتســهيل إدخــال الأوامر تقدم قشرة بــاش بعضاً من رموز البــدل الموضحة في الجدول (٣-٣). ورموز البدل المتوفرة هي: , ،و[..]، و *. وتقوم قشرة باش بتوســيع الكلمات التي تحتوي على هذه الرموز عن طريق استبدال الكلمة بقائمة من الملفات أو الأدلة التي تتفق مع عامل التصفية الذي أنشأه رمز البدل.

```
[alice@sunshine ~]$ cd /opt/book/system-admin/shell_expansion
[alice@sunshine shell_expansion]$ ls
goodbye.doc  heap.txt  helicopter.txt  hello.doc hello.txt help.txt
[alice@sunshine shell_expansion]$ ls *.doc
goodbye.doc  hello.doc
[alice@sunshine shell_expansion]$ ls he?p.txt
heap.txt  help.txt
```

إدارة الملفات:

تعلمت ســابقاً كيفية التنقل في نظام الملفات، وستتعلم الآن كيف تُجري تعديلات على الملفات والمجلدات.

إنشاء وحذف الأدلة:

لإنشاء وحذف الأدلة نستخدم الأمر (mkdir) والأمر (rmdir).

```
[alice@sunshine ~]$ cd /opt/book/system-admin/work
[alice@sunshine work]$ mkdir new_directory
```

```
[alice@sunshine work]$ ls -aF
./  ../ new_directory/
[alice@sunshine work]$ rmdir new_directory/
[alice@sunshine work]$ ls -aF
./  ../
```

يعمل الأمر (rmdir) فقط في الأدلة الفارغة. وستصلك رسالة بحدوث خطأ عندك محاولتك تشغيل هذا الأمر على دليل يحتوي ملفات و/أو مجلدات.

الجدول (٣-٣): رموز البدل في قشرة باش

رمز البدل	عامل التصفية	مثال
?	يقوم هذا الرمز بمطابقة رمز واحد أو لا رمز بكل الرموز	(re?d) تطابق (red)، و(reed)، و(read) لكنها لا تطابق (reads)
[..]	يحتوي هذا الرمز على قائمة أو مجال من الحروف/الأرقام التي يجب مطابقتها	(re[a,e]d) تطابق (reed)، و(read)، لكنها لا تطابق (red)
*	يقوم هذا الرمز بمطابقة رمز واحد أو أكثر بكل الرموز	(re*) تطابق (red)، و(reed)، و(read)

نسخ ونقل الملفات:

لنسـخ الملفات اسـتخدم الأمر (cp)، ولنقل الملفات من مجلد إلى آخر اسـتخدم الأمر (mv). ولتغيير اسـم الملف انقله فقط من اسـم الملف القديم إلى اسـم الملف الجديد. وتكون الصياغة كالتالي: <cmd> <source> <target>

```
[alice@sunshine work]$ cp ../shell_expansion/hello.txt hello_world.txt
[alice@sunshine work]$ ls -aF
./  ../  hello_world.txt
[alice@sunshine work]$ mv hello_world.txt HELLOWORLD.TXT
[alice@sunshine work]$ ls -aF
./ ../   HELLOWORLD.TXT
```

واضافة مفتاح (r-) (التكرارية) تسمح للأمر (cp) أن يعمل مع الأدلة ومع الملفات أيضاً. أما الأمر (mv) فهو يعمل بشكل تكراري دائماً. والتكرارية هي تحديد وظيفة اعتماداً على ما تقوم به تلك الوظيفة.

```
[alice@sunshine work]$ cd ~
[alice@sunshine ~]$ ls -F
Desktop/  Documents/  Music/  Pictures/  Public/  Videos/
[alice@sunshine ~]$ cp -r Documents/ Documents-copy
[alice@sunshine ~]$ ls -F
Desktop/   Documents/   Documents-copy/  Music/   Pictures/  Public/ Videos/
[alice@sunshine ~]$ mv Documents-copy Documents-moved
[alice@sunshine ~]$ ls -F
Desktop/ Documents/ Documents-moved/ Music/ Pictures/ Public/ Videos/
[alice@sunshine ~]$ ls -aF Documents
./ ../   notes.txt  readme  sample_file.mp٣
[alice@sunshine alice]$ ls -aF Documents-moved/
./ ../   notes.txt  readme  sample_file.mp٣
```

وكما ترى فإنه تم أولاً نسـخ دليل ملف المستندات (/Documents) بجميع محتوياته إلى الدليـل (/Documents-copy) ومـن ثم تم نقله إلى الاسـم الجديد (-Documents moved/). وتم تغيير اسم الدليل لكن المحتويات لم تتأثر بذلك.

حذف الملفات:

لحذف الملفات استخدم الأمر (rm).

[alice@sunshine ~]$ **cd Documents-moved/**

[alice@sunshine Documents-moved]$ **ls -aF**

./ ../ notes.txt readme sample_file.mp3

[alice@sunshine Documents-moved]$ **rm notes.txt**

[alice@sunshine Documents-moved]$ **ls -aF**

./ ../ readme sample_file.mp3

وللمساعدة في منع الحذف غير المقصود للبيانات قم باستخدام مفتاح (-i) مع الأوامر (cp)، و (mv)، و(rm). وسيُطلب منك التأكيد قبل حذف الملفات والتأكيد قبل نسخ/ نقل ملف يتطلب الكتابة على ملف موجود.

[alice@sunshine Documents-moved]$ **rm -i readme**

rm: remove regular file 'readme'? n

[alice@sunshine Documents-moved]$ **cp -i sample_file.mp3 readme**

cp: overwrite 'readme'? n

[alice@sunshine Documents-moved]$ **ls -aF**

./ ../ readme sample_file.mp3

الحذف التكراري:

كما هو الحال مع أمر (cp) فإن المفتاح التكراري (r-) يمكن اســتخدامه مع الأمر (rm) لحذف الأدلة، لكن اســتخدام المفتاح التكراري مــع الأمر (rm) ربما يكون أكثر خطورة لأن (rm-r) تعمل أولاً بحذف كل ملف في الدليل، ثم تقوم بحذف الدليل نفســه. وينبغي أن يكون احتمال وقوع كارثة واضح هنا. دائماً افحص وراجع المســار الذي قمت بإدخاله عند استخدامك (rm-r).

```
[alice@sunshine ~]$ ls -F
Desktop/  Documents/  Documents-moved/  Music/  Pictures/  Public/ Videos/
[alice@sunshine ~]$ rm -r Documents-moved/
[alice@sunshine ~]$ ls -F
Desktop/  Documents/  Music/  Pictures/  Public/  Videos/
```

عرض الملفات:

حتى الآن يمكنك أن تعرف مكانك في ملف النظام وأن تنقل الأشياء من حولك وأن تغير مالكها، لكن كيف يمكنك معرفة ما بداخل الملف؟ الغالبية العظمي من الملفات على خادم لينكس هي ملفات نصية لذا يمكن عرضها باستخدام عدد قليل من الأوامر البسيطة.

الأمر (LESS):

يسمح لك الأمر (less) بعرض الملفات النصية على الشاشة دفعة واحدة.

```
[alice@sunshine ~]$ less /usr/share/doc/openssl-1.0.0/FAQ
```

ويوضح الجدول (٣-٤) المفاتيح التي يمكنك استخدامها للتنقل والبحث في الملف. وعند استخدام هذا الأمر سيتم تظليل مصطلح البحث، وسوف ينتقل الملف إلى الأسفل حتى أول ظهور لمصطلح البحث والذي سيظهر أيضاً في أعلى وحدتك الطرفية.

الأوامر (HEAD) و (TAIL):

إذا كنت بحاجة فقط لرؤية بضعة أســطر من بداية أو نهاية الملف، اســتخدم (head) و (tail). ويتحكم المفتاح (n-) في عدد الأســطر التي ســيتم عرضها حيث إن عدد الأسطر الافتراضي عشرة أسطر.

```
[alice@sunshine ~]$ head /etc/passwd
root:x:0:0:root:/root:/bin/bash
bin:x:1:1:bin:/bin:/sbin/nologin
daemon:x:2:2:daemon:/sbin:/sbin/nologin
adm:x:3:4:adm:/var/adm:/sbin/nologin
lp:x:4:7:lp:/var/spool/lpd:/sbin/nologin
```

الجدول (٣-٤): الاختصارات الشائع استخدامها بلوحة المفاتيح (وتستخدم أيضاً مع الأمر less)

الأمر	الوصف
السهم السفلي	انتقل سطر واحد إلى الأمام
السهم العلوي	انتقل سطر واحد إلى الخلف
مفتاح المسافة	انتقل شاشة كاملة إلى الأمام
b	انتقل شاشة كاملة إلى الخلف
g	انتقل إلى بداية الملف
G	انتقل إلى نهاية الملف
pattern/	ابحث عن هذا النمط من الموقع الحالي إلى نهاية الملف
pattern?	ابحث عن هذا النمط من الموقع الحالي إلى بداية الملف
n	انتقل بالملف إلى حدوث التوافق القادم
N	انتقل بالملف إلى حدوث التوافق السابق
q	إنهاء

ملاحظة: بعض هذه الاختصارات تم ترحيلها إلى البريد الإلكتروني (Gmail). مثلاً أثناء قراءة البريد الإلكتروني فإن الأمر (typing/) سينقل المؤشر إلى مربع البحث[(٧)].

```
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
halt:x:7:0:halt:/sbin:/sbin/halt
mail:x:8:12:mail:/var/spool/mail:/sbin/nologin
uucp:x:10:14:uucp:/var/spool/uucp:/sbin/nologin
[alice@sunshine ~]$ tail -n5 /etc/group
sales_grp:x:504:
engineering_grp:x:505:
marketing_grp:x:506:
eric:x:507:
accounting_grp:x:508:
```

البحث عن الملفات:

يحتــوي خادم لينكس القيــاسي على آلاف الملفات، والبحث عــن ملف واحد بالتحديد يبدو كالبحث عن إبرة في كومة قش. ولكن يوجد أداة بحث قوية جداً للمساعدة في هذا الموضوع وهي الأمر (find). وفي أبســط أشــكاله يأخذ هذا الأمر شــكلين رئيسين: الدليل الذي يجب بدء البحث منه، واسم الملف الذي تبحث عنه. وهنا مثال عن البحث عن ملف ضبط أباتشي (Apache) (خادم الشبكة):

```
[alice@sunshine ~]$ find /etc -name httpd.conf
/etc/httpd/conf/httpd.conf
```

(7) http://support.google.com/mail/bin/answer.py?hl = en&answer = 6594

وكما تُلاحظ فإن الأمر (find) يستخدم صياغة تختلف عن صياغة بقية الأوامر السابقة والتي عملنا عليها حتى الآن إذ إن مفتاح الأمر يتبع اسم الأمر في جميع تلك الأوامر. لكن مــع الأمر (find) فإن الطريقة تختلــف حيث يأتي مفتاح (-name) بعد العنصر الأول (/). ويشــير كُتيب إرشــادات الأمر (find) إلى أن المفتاح التالي (-name httpd.conf) هو جزء مــن الأمر(find)، كما يُعد هذا المفتاح بأنه مصطلــح (Expression). وهناك العديد من العوامل التي يمكن استخدامها على أنها مصطلح مثل (-user) (والذي يقوم بإيجاد الملفات التابعة لحساب محدد)، أو (-empty) (والذي يقوم بإيجاد الملفات الفارغة). ويمكن أيضاً دمج مصطلحات متعددة لتضييق نتائج البحث:

```
[alice@sunshine ~]$ find /opt -user alice -empty
/opt/book/system-admin/my_file.txt
```

التحكم في الوصول وإدارة المستخدم:

الأذونات:

يتحكــم نظام لينكــس ومعظم أنظمة التشــغيل المُعتمِدة على ينكــس في الوصول إلى الملفــات مــن خلال آليتين: أذونات الملفات، وقوائم التحكــم في الوصول. أذونات الملفات هي الطريقة التقليدية للتحكم في الوصول إلى الملفات والتي تم استخدامها منذ الأيام الأولى لنظــام ينكــس. وهذه الأذونات مدعومة بشــكل كامل من أوامر القــشرة، كما أنها تعمل بثبات مع أنظمة التشــغيل المُختلفة. أما قوائم التحكم في الوصول فهي أكثر حداثة وأكثر دقة في ضبط التحكم حيث تتحكم في الذين يمكنهم الوصول إلى الملفات، وتتحكم أيضاً فيما يمكنهم القيام بعمله في هذه الملفات. ولسوء الحظ هناك توحيد متواضع لتطبيقات قوائم التحكم في الوصول في أنظمة التشغيل المختلفة، كما أن هناك أدوات دعم محدودة. لذلك يتــم عادة تفضيل أذونات الملفات أكثر من قوائم التحكم في الوصول. وســوف نســتعرض هاتين الآليتين مع التركيز أساســاً على أذونات الملفات، لكن سنشرح فوائد الميزات الإضافية لقوائم التحكم في الوصول.

أمر (LS) مرة أخرى:

اســتخدم مفتاح (-l) مع أمر (ls) لعرض أذونات الملف الحالية حيث يقوم هذا المفتاح بعرض قوائم الدليل في الهيئة المطولة المقســمة إلى ســبعة أعمدة. ويوضح الجدول (٣-٥) وصف الأعمدة في قوائم الملفات المطولة.

```
[alice@sunshine ~]$ cd /home/shared
[alice@sunshine shared]$ ls -laF
total 56
drwxr-xr-x.   5 root root       4096  Jan 29  2012 ./
drwxr-xr-x.  12 root root      36864  Feb 15 19:57 ../
drwxr-xr-x.   6 root root       4096  Jan 29  2012 academic_affairs/
drwxr-xr-x.   5 root root       4096  Jan 29  2012 business_finance/
drwxr-xr-x.   2 root legal_grp  4096  Jan 29  2012 legal/
```

الجدول (٣-٥): وصف الأعمدة في قوائم الملفات المطولة

مكان العمود	الوصف	مثال
١	أذونات الملفات/الأدلة	drwxr-xr-x
٢	عدد الروابط الثابتة لنظام الملفات	٢
٣	ملكية المستخدم للملف/الدليل	Root
٤	ملكية المجموعة للملف/الدليل	engineering_grp
٥	حجم الملف/الدليل بالبايت	٤٠٩٦
٦	تعديل الطابع الزمني	Jan 28 19:06
٧	اسم الملف/الدليل	/engineering

التدوين الرمزي:

الآن سنلقي نظرة فاحصة على أذونات الملفات/الأدلة في العمود الأول. ويقدم الأمر (ls -l) أذونات الملف بالتدوين الرمزي[٨]. وللمزيد من الأمثلة انظر الجدول (٣-٧).

الرمز الأول يشير إلى نوع الملف:

d Directory دليل

- Regular file ملف عادي

b Block/special file رزمة/ ملف خاص

c Character/special file رمز/ ملف خاص

l Symbolic link رابط رمزي

p Named pipe انبوبة اتصال مسماة

s Socket القابس

وتم تقسيم الرموز التسعة التالية إلى ثلاث مجموعات وكل مجموعة تتكون من ثلاثة رموز:

١. ما يستطيع أن يفعله المالك

٢. ما يستطيع أن يفعله أعضاء المجموعة المالكين للملف

٣. ما يستطيع جميع المستخدمين (العالم) فعله

وتم توزيع كل مجموعة في ثلاثة أعمدة:

r- Read قراءة

w- Write كتابة

x- eXecute تنفيذ

(8) http://en.wikipedia.org/wiki/Filesystem_permissions#Symbolic_notation

وبالإضافة إلى التنفيذ فإن العمود الثالث يمثل أيضاً مواصفات خاصة يمكن تطبيقها على الملف:

(s – setuid/setgid) بدلاً من استخدام أذونات المستخدم لتنفيذ الملف، فإن هذا الملف سيعمل وكأنه المالك (setuid) أو كأنه المجموعة (setgid) بناءً على ما يتم تحديده في هذا الأمر.

(T – sticky bit) عند ضبط هذه الخاصية في الدليل، فإن أي مستخدم لديه صلاحية الكتابة يُمكنه إنشاء ملفات في هذا الدليل، لكن المالك فقط يستطيع نقل أو حذف تلك الملفات.

الترميز الثماني:

وبالإضافة إلى التدوين الرمزي فإن بعض الأوامر تستخدم الترميز الثماني لتمثيل أذونات الملفات. ويتكون الترميز الثماني من ثلاثة أرقام (ثُمَانِيّة الأساس)، كل منها يمثل جزءاً من الأذونات: المستخدم، والمجموعة، والعالم. وتم احتساب القيم بإضافة ثلاثة بتات (bits) ثُمَانِيّة (انظر الجدول ٣-٦).

الجدول (٣-٦): الترميز الثماني

الثماني	الرمز	الوصف
٠	---	بدون اذونات
١	x--	تنفيذ
٢	-w-	كتابة
٣	wx-	كتابة/تنفيذ
٤	--r	قراءة
٥	r-x	قراءة/تنفيذ
٦	-rw	قراءة/كتابة
٧	rwx	قراءة/كتابة/تنفيذ

الجدول (٣-٧): أمثلة على أذونات الملفات

التدوين الرمزي	الترميز الثماني	التوضيح
d rwx r-x r-x	٧٥٥	دليل بأذونات قراءة/ كتابة/ تنفيذ للمالك، وأذونات قراءة/ تنفيذ للمجموعة وللعالم
- r -rw-- ---	٦٤٠	ملف عادي بأذونات قراءة/ كتابة للمالك، وأذونات قراءة للمجموعة، وبدون أذونات للعالم

١. بت القراءة (read bit) تضيف ٤ إلى المجموع (ثنائي: ١٠٠)

٢. بت الكتابة (write bit) تضيف ٢ (ثنائي: ٠١٠)

٣. بت التنفيذ (execute bit) تضيف ١ (ثنائي: ٠٠١)

تغيير الأذونات:

يُستخدم الأمر (chmod) لتغيير أذونات الملف أو الدليل، حيث يستخدم هذا الأمر الترميز الثماني عند إدخال الأذونات. وفي المثال القادم سنقوم بتغيير أذونات الدليل (/home/shared/legal) لإعطاء مالك الدليل أذونات بالقراءة والكتابة والتنفيذ، وإعطاء كل شخص في مجموعة (legal_grp) أذونات بالقراءة والكتابة والتنفيذ، وإعطاء كل شخص آخر أذونات بالقراءة والتنفيذ.

> العديد من الأوامر التالية يجب تشغيلها بامتيازات مستخدم ذو صلاحيات كاملة. واسم المستخدم للحساب ذو الصلاحيات الكاملة هو (root) وهو من أقوى الأسماء الإدارية في أنظمة التشغيل المُعتمدة على نظام ينكس. ويتمكن المُستخدم ذو الصلاحيات الكاملة من عرض وتعديل وحذفَ أي ملف في النظام. ويجب أن يتم الوصول لحساب المستخدم ذي الصلاحيات الكاملة بحذر شديد. وسنناقش فيما بعد كيف يتم مشاركة بعض من هذه الامتيازات مع حسابات مستخدمين آخرين. لكن الآن سنقوم بتحويل حسابات المستخدمين باستخدام الأمر (su)، وكذلك استخدام الحساب ذو الصلاحيات الكاملة.

[alice@sunshine shared]$ **su -**

Password: **thisisasecret**

[root@sunshine ~]#

لاحــظ أن موجه الأوامر قد تغير حيث يظهر اســم المســتخدم الحــالي (root) وعلامة الدولار ($) تم استبدالها برمز المربع (#). ويتم استخدام علامة المربع بموجه الأوامر الخاص بـــ (root) في كثير من أنظمة التشــغيل والعديد من أنواع القشرة. لــذا عندما تراها لابد أن تكــون حــذراً للغاية مع الأوامر التي تكتبها لأن أي خطأ بســيط ممكن أن يكون كارثياً خصوصاً عند استخدام الحساب ذي الصلاحيات الكاملة.

```
[root@sunshine ~]# [cd /home/shared
[root@sunshine shared]# [ls -laF
total 56
drwxr-xr-x.   5 root root       4096 Jan 29  2012  ./
drwxr-xr-x.  12 root root      36864 Feb 15 19:57  ../
drwxr-xr-x.   6 root root       4096 Jan 29  2012  academic_affairs/
drwxr-xr-x.   5 root root       4096 Jan 29  2012  business_finance/
drwxr-xr-x.   2 root legal_grp   4096 Jan 29  2012  legal/
-rw-r--r--   1 root root       3969 May 29 10:20  README
[root@sunshine shared]# [chmod 775 legal
[root@sunshine shared]# [ls -laF
total 56
drwxr-xr-x.   5 root root       4096 Jan 29  2012  ./
drwxr-xr-x.  12 root root      36864 Feb 15 19:57  ../
drwxr-xr-x.   6 root root       4096 Jan 29  2012  academic_affairs/
drwxr-xr-x.   5 root root       4096 Jan 29  2012  business_finance/
drwxrwxr-x.   2 root legal_grp   4096 Jan 29  2012  legal/
-rw-r--r--   1 root root       3969 May 29 10:20  README
```

الآن تـم تغيير الأذونات على دليل (legal) مـن (drwxr-xr-x) إلى (drwxr-wxr-x). وبعبارة أخرى تم إضافة إذن الكتابة في هذا الدليل إلى المجموعة.

قوائم التحكم في الوصول:

تتميـز الأذونات الموحدة في ملـف ينكس بالقوة، لكن نقطة ضعفهـا الوحيدة أنه كل ملـف يمكن أن يملكه مسـتخدم واحد ومجموعة في الوقت نفسـه. إذا كان لديك العديد من الأشـخاص الذين يحتاجون لمسـتويات مختلفة من الوصول لملـف معين فإن أذونات ملـف ينكس لن تكـون كافية. عندها يجب الاسـتفادة من (قوائـم التحكم في الوصول) والموجودة في مُعظم أنظمة تشـغيل ينكـس الحديثة. ونوضح ذلك بمثال: لنقل إنك تريد أن تسـمح لاثنين من المسـتخدمين بوصول القراءة والكتابة لملف ما، وفي الوقت ذاته تريد أن تسـمح لمجموعة منفصلة بوصول القراءة فقط، بينما بقية المستخدمين يجب ألا يُسمح لهم بالوصول لهذا الملف. وهذا لن يكون ممكناً باسـتخدام أذونات الملف الموحدة، لكنه سيكون سهلاً باستخدام أمر (setfacl).

```
[root@sunshine ~]# cd /opt/book/system-admin/access_control

[root@sunshine access_control]# ls -laF

total 52

drwxr-xr-x  5 root root       4096 Jan 29  2012 ./

drwxr-xr-x 12 root root      36864 Feb 15 19:57 ../

-rw-r--r--  1 root root      43836 May 29 10:06 document.txt

[root@sunshine access_control]# chmod 600 document.txt

[root@sunshine access_control]# ls -laF document.txt

-rw-------  1 root root      43836 May 29 10:06 document.txt

[root@sunshine access_control]# setfacl -m u:alice:rw document.txt
```

```
[root@sunshine access_control]# setfacl -m u:bob:rw document.txt
[root@sunshine access_control]# setfacl -m g:legal_grp:r document.txt
[root@sunshine access_control]# setfacl -m o-:  document.txt
```

ويأخـــذ الأمر (setfacl -m) معاملـــين: الأول يقوم بتطبيق (قوائم التحكم في الوصول)، والثـــاني هو الملف الذي يجب تطبيق (قوائم التحكم في الوصول) عليه. والإدخال مُقســـم إلى ثلاثة حقول مفصولة بعلامة النقطتين (:). الحقل الأول يشـــير إلى نوع الإدخال في قائمة التحكم في الوصول:

Useru- مستخدم- تعديل الوصول للملف لمستخدم واحد

Groupg- تعديل الوصول للملف لمجموعة من المستخدمين

Otherso- تعديل الوصول للملف لجميع المستخدمين الذين لم يتم منحهم حق الوصل من خلال قائمة التحكم في الوصول للمستخدم أو للمجموعة

الحقـــل الثـــاني يحدد الذين تنطبق عليهـــم (قائمة التحكم في الوصـــول). في حالة قائمة التحكم في الوصول للمســـتخدم أو للمجموعة، فإن هذا الحقل ســـيكون اسم المستخدم أو المجموعـــة على التوالي. وفي حالة تطبيـــق قائمة التحكم في الوصول على الآخرين (others) فإن هذا الحقل سيكون فارغاً.

وأخيراً فإن الحقل الثالث يحتوي على قائمة الأذونات التي يجب أن تمنح من خلال قائمة التحكم في الوصول. وبشـــكل مشابه للأمر (chmod) فإن الأمر (setfacl) يستخدم الترميز الثماني للتعبير عن وصول القراءة (r)، والكتابة (w)، والتنفيذ (x).

ويقوم الأمر (getfacl) بسرد (قوائم التحكم في الوصول) التي تم وضعها في الملف.

```
[root@sunshine access_control]# getfacl document.txt
# file:  document.txt
# owner:  root
```

```
# group:  root
user::rw-
user:alice:rw-
user:bob:rw-
group::---
group:legal_grp:r--
mask::rw-
other::---
```

وبإمكانك أن ترى نتيجة تطبيق (قائمة التحكم في الوصول) إلى الملف باستخدام الأمر (ls -l)

```
[root@sunshine access_control]# ls -laF document.txt
-rw-------+ 1  root root      43836   May  29 10:06 document.txt
```

إشارة الزائد (+) في العمود الأخير من الأذونات تُشير إلى وجود (قوائم التحكم في الوصول).

ملكية الملف:

سنُلقي الآن نظرة أخرى على مخرجات الأمر (ls –l).

```
[root@sunshine ~]# cd /home/shared
[root@sunshine shared]# ls -laF
total 56
drwxr-xr-x.   5 root root       4096 Jan 29   2012  ./
drwxr-xr-x.  12 root root      36864 Feb 15  19:57  ../
drwxr-xr-x.   6 root root       4096 Jan 29   2012  academic_affairs/
```

```
drwxr-xr-x.   5 root root        4096 Jan 29   2012  business_finance/
drwxr-xr-x.   2 root legal_grp  4096 Jan 29   2012  legal/
-rw-r--r--   1 root root        3969 May 29  10:20  README
```

ويُخبر العمود الثالث عن مالك الملف وهو المســتخدم الذي أنشــأ الملف، أو المستخدم الذي تم تحويل ملكية الملف إليه من المالك الســابق أو من مســؤول النظام. وبالمثل فإن العمود الرابع يحدد المجموعة التي تملك الملف. وعادةً هذا هو الوضع الافتراضي لمجموعة المســتخدم الذي أنشأ الملف. ومع ذلك ســنتعلم لاحقاً في هذا الفصل ما يؤثر في استخدام المجموعة الافتراضية.

تغيير الملكية:

يتــم تغيير ملكية شــخص أو ملكية مجموعــة لملف ما من خــلال الأمرين (chown) و(chgrp) على الترتيب. وفي هذا المثال سنقوم بتغيير ملكية (home/share/README/) إلى المستخدم (dave) وإلى المجموعة (library_grp).

```
[root@sunshine shared]# cd /home/shared
[root@sunshine shared]# chown dave README
[root@sunshine shared]# chgrp library_grp README
[root@sunshine shared]# ls -laF
total 56
drwxr-xr-x.   5 root root         4096 Jan 29  2012 ./
drwxr-xr-x.  12 root root        36864 Feb 15 19:57 ../
drwxr-xr-x.   6 root root         4096 Jan 29  2012 academic_affairs/
drwxr-xr-x.   5 root root         4096 Jan 29  2012 business_finance/
drwxr-xr-x.   2 root legal_grp    4096 Jan 29  2012 legal/
-rw-r--r--   1 dave library_grp  3969 May 29 10:20 README
```

تحرير الملفات:

يمكنــك رؤية محتويات الملف، وتحتــاج الآن إلى معرفة كيفية إنشــاء وتحرير الملفات بنفســك. وهناك المئات من البرامج المتوفرة لتحرير الملفات[٩] بدءاً من أبسطها وهو مُحرر نص سطر الأوامر (command-line text editor) وصولاً إلى البرامج الرسومية التي تنافس مايكروسوفت وورد في المواصفات. لكنك خلال حياتك المهنية ستستخدم العديد من أنواع وإصدارات أنظمة التشغيل المُعتمِدة على نظام ينكس، وقد لا يكون برنامج التحرير المفضل لديــك متوفــراً في كلٍ منهم. هناك مُحــرر واحد فقط موجود في جميع أنظمة التشــغيل المُعتمدة على نظام ينكس وهو المُحرر (في-آي) (vi editor).

المُحرر السادس:

أول شيء عليك تعلمه هو كيفية نطق اســم المحرر. لا تحاول أن تنطق الاســم ككلمة (vie) ولا تقــم بقراءتــه على أنه الرقم الروماني ســتة (vi). عليك فقط أن تنطق كل حرف منفرداً (في-آي) (vee-eye). أيضاً فإن مُســتخدمي ينكس عادة يســتخدمون (vi) على أنها فعل (في-آي هذا الملف) وليس على أنها اسم (افتح هذا الملف في محرر في-آي).

كُتِب محرر (في-آي) (vi) بواسطة بل جوي في عام ١٩٧٦ وأصبح جزءاً أساسياً من نظام تشغيل ينكس منذ إطلاقه مع توزيعة برمجيات بيركلي (BSD) في عام ١٩٧٦. ومنذ ذلك الحين مرّ هذا المحرر بالعديد من التغييرات وإعادة الكتابة، وقد تم تحويله (إعادة كتابته ليعمل على أجهزة وأنظمة تشغيل أخرى) إلى جميع أنظمة التشغيل التي تم إصدارها في ذلك الوقت. ولأنه موجود في العديد من الأنظمة فإن محرر (في-آي) هو المعيار العملي لتحرير النصوص. ومع أنه تم إضافة العديد من المميزات للإصدارات المختلفة من محرر (في-آي) إلا أنه يحتوي على مجموعة موحدة من المهام التي تطبقها جميع الإصدارات. وسيبقى هذا الكتاب ضمن تلك المهام الموحدة، ولكن سيتم وضع جميع الأمثلة من الإصدار الرئيسي لمحرر (في-آي) المُستخدم في نظام ينكس (في-آي المُحسن).

(9) http://freecode.com/search?q = text+editor&submit = Search

أساسيات محرر (في-آي):

ينتاب الكثير من الأشــخاص حالة من الخوف عندمــا يفتحون محرر (في-آي) لأول مرة حيث لا يحتوي هذا المحررٍ على قوائم أو على مســاعدة من أي نوع، وبشــكل عام يعرض المحرر معلومات قليلة جداً. ولمساعدة الأشخاص الذين يستخدمون المحرر لأول مرة فلقد تم تصميم برنامج تعليمي يُدعى (vimtutor). ويقوم هذا البرنامج التعليمي بعرض جميع الوظائف الأساســية للمحرر، كما يقوم بتقديم المميزات التي تجعل من المحرر أداة لا غنى عنها حتى بعد مرور ٣٥ عاماً من بدء تطوير هذا المحرر. وحتى تكتمل فائدتك الشخصية ننصح بشدة أن تقوم بالاطلاع على البرنامج التعليمي الـ (vimtutor)[١٠].

[alice@sunshine ~]$ **vimtutor**

وسيقوم هذا الأمر بتشغيل البرنامج التعليمي (vimtutor) كما هو مبين في الشكل (٣-٤).

محرر (في-آي) والجيميل (Gmail)

الكثير من المستخدمين لا يعلمون عن العديد من اختصارات لوحة المفاتيح المتاحة في جيميل (Gmail)[١١]. وبعد فحص دقيق يتضح أن بعضاً من هذه الاختصارات مستوحاة من الاختصارات المقابلة في محرر (في-آي). ومن الأمثلة على ذلك: (/) للبحث، و(k) للانتقال إلى محادثة أحدث، (j) للانتقال إلى محادثة أقدم.

تثبيت البرمجيات والتحديثات:

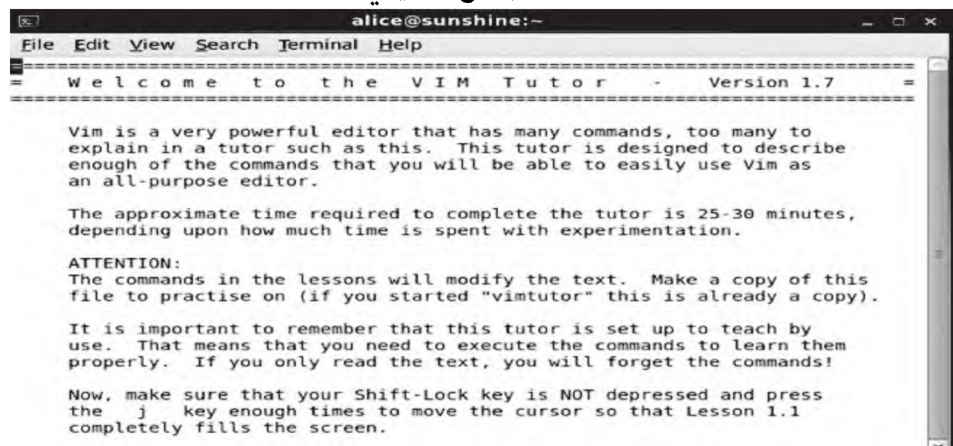
في عــالم لينكس تُســمى التطبيقات غالبــاً بالحزم (packages). ويعــد تثبيت البرامج الجديــدة، والمحافظــة عــلى ترقية حزم البرمجيــات الموجودة في جميع الخــوادم من أهم الوظائف اليومية للمســؤول عن النظام. ويمكن أن يشكل هذا تحدياً بسبب العدد الهائل للحزم التي تشكل نظام التشغيل التقليدي للخادم. وحتى أن تثبيت نظام أولي من أنظمة لينكس، كالمُستخدم في تمارين هذا الكتاب، يشتمل على أكثر من ألف من الحزم المنفصلة.

(١٠) انظر اختصارات لوحة المفاتيح لمحرر (في-آي) على الموقع: http://www.viemu.com/a_vi_vim_graphical_cheat_sheet_tutorial.html

(11) http://support.google.com/mail/bin/answer.py?hl = en&answer = 6594



شكل (٣-٤): واجهة البرنامج التعليمي (vimtutor)



تهيئة الحزَم:

إذا لم تعمل مُســبقاً مع أنظمة التشغيل المُعتمِدة على نظام ينكس فإن حزَم البرمجيات ليســت مألوفة لديك. ففي نظام مايكروسوفت ويندوز ونظام ماك أو أس إكس، يتم عادة توزيع تحديثات نظام التشــغيل كحزَم كبيرة والتي تقــوم بتحديث العديد من أجزاء نظام التشــغيل في وقت واحد. وبالمثل فإن تحديث التطبيقات على هذه الأنظمة الأساسية يتم توزيعها في ملف تثبيت واحد والذي يحل محل العديد من ملفات الاصدار القديم.

ويقــوم نظام لينكــس، ومعظم أنظمة التشــغيل الأخرى المُعتمدة عــلى نظام ينكس، بتوزيع تحديثات نظام التشــغيل والتطبيقات على شكل حزَم برمجيات. وبدلاً من تحزيم كافة الملفات التي يحتاج إليها التطبيق في ملف واحد، يتم تقســيم التطبيقات إلى مكونات أصغر يمكن اســتخدامها من قِبل تطبيقات أخرى. ويتم تحويل هذه المكونات الصغيرة إلى حزَم البرمجيات. وكل حزمة تحتوي على قائمة من التوابع، وهي الحزَم التي يجب أن تُثبَت قبل أن يتم تثبيت هذه الحزمة بشــكل صحيح. ويمكن أن تُصبح قوائم التوابع تلك شاملة حتى للتطبيقات التي تبدو إلى حد ما بسيطة. وكمثال على ذلك أدخل هذا الأمر لترى قائمة التوابع لمتصفح الفايرفوكس. سترى أن فايرفوكس يعتمد على العديد من الحزَم الأخرى:

```
[alice@sunshine ~]$ repoquery --requires firefox
```

مدير حزمة الـ (YUM):

يتضمـــن نظـــام ســـينتوس لينكـــس (CentOS Linux) على مدير حزمـــة الـ (YUM) لمســـاعدة مســـؤول النظام في مهام تثبيت الحزم الجديدة، ومتابعة قوائم التوابع، وتحديث الحـــزَم. ويعمل (YUM) عن طريق بناء قاعدة بيانات لحُـــزم الـ (RPM) المثبتة حالياً في النظـــام، ومن ثم مقارنتها بمســـتودعات الحزَم الموجودة في الإنترنـــت على مواقع بروتوكول نقـــل النص التشـــعبي (HTTP) ومواقع بروتوكول نقل الملفـــات (FTP) التي تحتوي على جميـــع الحـــزَم التي تم إصدارها. ولضمان أن مســـتودعات الحزَم تكـــون دائماً مُتاحة وأنه يمكن تحميل الحَزم بسرعة يتم نســـخ الملفات بين المئات من الخوادم حول العالم[١٢]. وكل منها يعد «مرايا» للمســـتودع الرئيسي وتحتوي على كافة الملفات الأصلية ويمكن استخدامها لجميع إجراءات التثبيت والتحديث. وقبل تحميل أي ملف يقوم (YUM) تلقائياً باختبار سرعة التحميل للمرايا المُتاحة ومن ثم اختيار المرايا الأسرع.

الأوامر (YUM INSTALL) و(YUM REMOVE):

يقـــوم الأمـــر (YUM INSTALL) بتحميل الحزمة المطلوبة وكذلـــك الحزم التابعة لها من مســـتودعات الحزَم. وكمثال على ذلك سنقوم بتثبيت حزمة ألعاب (gnome-games) والتي تضم عدداً قليلاً من الألعاب مثل السوليتير (Solitaire) وسودوكو (Sudoku).

```
[root@sunshine ~]# yum install gnome-games
Loaded plugins:  fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base:  mirrors.gigenet.com
 * extras:  mirrors.gigenet.com
 * updates:  centos.mirror.choopa.net
Setting up Install Process
Resolving Dependencies
```

(12) http://www.centos.org/modules/tinycontent/index.php?id = 30

```
--> Running transaction check
---> Package gnome-games.i686 1:2.28.22-.el6 will be installed
[Output shortened to conserve space]
Dependencies Resolved
=========================================================
======================================
 Package        Arch           Version
Repository       Size
=========================================================
======================================
Installing:
 gnome-games     i686            1:2.28.22-.el6          base
3.3 M
Installing for dependencies:
 clutter         i686            1.0.63-.el6             base
320 k
 ggz-base-libs   i686            0.99.55.1-.el6          base
189 k
 guile           i686            5:1.8.75-.el6           base
1.4 M
Transaction Summary
=========================================================
======================================
```

```
Install       4 Package(s)
Total download size:  5.1 M
Installed size:  18 M
Is this ok [y/N]:  y
Downloading Packages:
(14/):  clutter-1.0.63-.el6.i686.rpm
| 320 kB     00:00
(24/):  ggz-base-libs-0.99.55.1-.el6.i686.rpm
| 189 kB     00:00
(34/):  gnome-games-2.28.22-.el6.i686.rpm
| 3.3 MB     00:03
(44/):  guile-1.8.75-.el6.i686.rpm
| 1.4 MB     00:01
--------------------------------------------------------------------
-----------------------
Total                                          744 kB/s
| 5.1 MB     00:07
[Output shortened to conserve space]
Installed:
  gnome-games.i686 1:2.28.22-.el6
Dependency Installed:
```

clutter.i686 0:1.0.63-.el6 ggz-base-libs.i686 0:0.99.55.1-.el6

guile.i686 5:1.8.75-.el6

Complete!

[root@sunshine ~]# **gnome-sudoku**

وفي هذا المثال تم إدراج ثلاثة مستودعات افتراضية للحزَم (base, extras, updates) إلى المرايا الأسرع التي تم اختيارها للمستودع. وبعد ذلك يقوم (yum) بتحميل قائمة الحزَم التابعة لألعاب (gnome-games) ومقارنة هذه القائمة بالحزَم المُثبتة مُسبقاً في النظام. ومن ثَمّ يتم عرض قائمة بجميع الحزَم التي سيتم تثبيتها على مسؤول النظام. وإذا كان مسؤول النظام يرغب بالاستمرار في العملية سيتم تثبيت الحزَم وسيكون التطبيق جاهزاً للاستخدام.

وإذا لم تعد هناك حاجة لحزمة ما فإن الأمر (yum remove) يقوم بحذف الحزمة وحذف أي حزَم أخرى تعتمد عليها. ومن الواضح أنه يجب توخي الحذر عند استخدام الأمر (yum remove) للتأكد من أن الحزَم الضرورية لعمل الخادم لن تتأثر.

[root@sunshine ~]# **yum remove gnome-games**

Loaded plugins: fastestmirror, refresh-packagekit, security

Setting up Remove Process

Resolving Dependencies

--> Running transaction check

---> Package gnome-games.i686 1:2.28.22-.el6 will be erased

--> Finished Dependency Resolution

Dependencies Resolved

===

===================================

```
 Package              Arch             Version
Repository      Size
 ==========================================================
=====================================
Removing:
 gnome-games            i686            1:2.28.22-.el6        @base
14 M
Transaction Summary
==========================================================
=====================================
Remove        1 Package(s)
Installed size:  14 M
Is this ok [y/N]:  y
Downloading Packages:
Running rpm_check_debug
Running Transaction Test
Transaction Test Succeeded
Running Transaction
  Erasing     :  1:gnome-games-2.28.22-.el6.i686
11/
Removed:
```

```
gnome-games.i686 1:2.28.22-.el6
Complete!
```

الأوامر (YUM LIST) و(YUM SEARCH):

لقد رأينا أن الأمر (yum install) يسمح لك بتثبيت الحزَم الجديدة، لكن كيف يمكنك معرفة الحــزَم الجاهزة؟ يقوم الأمر (yum list) بعرض جميع الحزَم الجاهزة، كما يســمح الأمــر (yum search) بالبحث عن الحزَم التي عنوانهــا و/أو وصفها يحتوي على مفردات البحث.

```
[root@sunshine ~]# yum list
Loaded plugins:  fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base:  mirrors.gigenet.com
 * extras:  mirrors.gigenet.com
 * updates:  centos.mirror.choopa.net
Installed Packages
ConsoleKit.i686             0.4.1–3.el6                @anaconda-
CentOS-201112130233.i3866.2/
ConsoleKit-libs.i686         0.4.1–3.el6                @anaconda-
CentOS-201112130233.i3866.2/
ConsoleKit-x11.i686          0.4.1–3.el6                @anaconda-
CentOS-201112130233.i3866.2/
[Output shortened to conserve space]
zlib-static.i686                      1.2.327-.el6
```

```
base
zsh.i686                     4.3.104.1-.el6
base
zsh-html.i686                  4.3.104.1-.el6
base
[root@sunshine ~]# yum search games
Loaded plugins:  fastestmirror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
 * base:  mirrors.gigenet.com
 * extras:  mirrors.gigenet.com
 * updates:  centos.mirror.choopa.net
=== N/S Matched:  games
==================================================
gnome–games.i686 :  Games for the GNOME desktop
gnome–games–extra.i686 :  More games for the GNOME desktop
gnome–games–help.noarch :  Help files for gnome-games
kdegames.i686 :  KDE Games
kdegames–libs.i686 :  Runtime libraries for kdegames
kdegames–devel.i686 :  Header files for compiling KDE 4 game
applications
```

الأمر (YUM UPDATE):

يوفر الأمر (yum update) طريقة سهلة لمسح جميع الحزَم المُثبتة على النظام، ومقارنة إصداراتهــا بأحدث الإصدارات المتوفــرة، كما يقدم تقريراً عن تلك الحــزَم التي تحتاج إلى تحديث.

```
[root@sunshine ~]# yum update
Loaded plugins:  fastestmirror, refresh-packagekit, security
Determining fastest mirrors
 * base:  mirrors.gigenet.com
 * extras:  mirrors.gigenet.com
 * updates:  centos.mirror.choopa.net
base                                    | 3.7 kB
00:00
extras                                  | 3.5 kB
00:00
updates                                  | 3.5 kB
00:00
updates/primary_db                          | 2.8 MB
00:03
Setting up Update Process
Resolving Dependencies
--> Running transaction check
---> Package firefox.i686 0:10.0.31-.el6.centos will be updated
```

```
[Output shortened to conserve space]
Transaction Summary
=====================================================
==========================
Install       1 Package(s)
Upgrade      23 Package(s)
Remove        1 Package(s)
Total download size:  92 M
Is this ok [y/N]:  y
Downloading Packages:
(124/):  firefox–10.0.4–1.el6.centos.i686.rpm          | 20 MB
00:24
(224/):  kernel–2.6.32–220.13.1.el6.i686.rpm           | 22 MB
00:30
(324/):  kernel–firmware–2.6.32–220.13.1.el6.noarch.    | 6.2 MB
00:07
(424/):  kpartx-0.4.9–46.el6_2.2.i686.rpm              | 45 kB
00:00
(524/):  libpng-1.2.491-.el6_2.i686.rpm                | 184 kB
00:00
[Output shortened to conserve space]
Complete!
```

وكما ستلاحظ أن تلك المخرجات مشابهة لمخرجات (yum install). ومن المُثير للاهتمام أيضاً ملاحظة أن أمر (yum update) يستطيع تثبيت وحذف الحزَم بالإضافة إلى تحديثها. وفي أثناء تطوير وتحديث حزَم البرمجيات قد يحدث تغيير في الحزَم التي تعتمد عليها أو قد يتم تغيير أسماء الحزَم مما يتطلب إزالة الحزَم القديمة واستبدالها بالحزَم الجديدة.

إدارة الحساب:

اعتماداً على البيئة التي يعمل فيها مسؤول النظام فإن إدارة الحساب قد تستغرق جزءاً كبيراً من وقت مسؤول النظام أو قد لا تأخذ إدارة الحساب أي وقت على الاطلاق. ويُعد عدد حسابات المستخدمين، ونسبة المستخدمين التي تتم إضافتها أو حذفها بمعدل منتظم بعضاً من العوامل التي تؤثر في كمية العمل في إدارة الحساب. وفي المنظمات الكبيرة كالجامعات والشركات الكبرى فإن مهام إدارة الحساب معقدة جداً وعدد تلك المهام كبير أيضاً بحيث يصعب معالجتها يدوياً. وفي هذه الحالات يتم استخدام حل إدارة الهوية (Identity Management) لتصميم قواعد إدارة الحساب التي يمكن تطبيقها آلياً لجميع المستخدمين الحاليين والمحتملين. وسوف نغطي إدارة الهوية بعمق أكبر في فصل قادم، لكن الآن سننظر في إجراءات إدارة الحساب اليدوية.

مدير المستخدم (User Manager):

إن أسهل طريقة لإدارة حسابات المستخدمين وعضوية المجموعة في سينتوس هي استخدام مدير المستخدم (User Manager) وهي أداة رسومية تأتي ضمن التثبيت التقليدي لسينتوس. ويمكنك تشغيلها عن طريق اختيار المجموعات والمستخدم (User and Groups) من قائمة الإدارة (Administration menu) كما هو موضح في الشكل (٣-٥).

وتشبه الواجهة إلى حد كبير صفحات إدارة المستخدم في نظام ويندوز (Windows) ونظام ماك أو إس إكس (Mac OSX) (الشكل ٣-٦). ولإضافة مستخدمة جديد انقر على زر إضافة مستخدم (Add User) وقم بتعبئة نموذج المستخدم الجديد. وبشكل افتراضي فإن الأداة ستنشئ دليل رئيسي للمستخدم في دليل (home/) الموجود في نظام الملفات، كما ستقوم الأداة بإصدار الارقام التعريفية المتاحة للمستخدمين والمجموعات. لكن يمكنك

تجاوز ذلك والقيام بإدخال قيم مخصصة إذا لزم الأمر. كما يمكنك أيضاً حذف المستخدم عن طريق اختيار زر حذف (Delete).

وأخيراً يمكنك تعديل حساب موجود بواسطة تحديد الحساب من القائمة والنقر على زر خصائص (Properties). وفي محرر الحساب تستطيع تغيير أي من مجموعة القيم عند إنشاء الحساب. بالإضافة إلى ذلك يمكنك تعديل بعض إعدادات تحكم الوصول للحساب مثل:

- انتهاء الحساب - بعد هذا التاريخ لن يكون الحساب قابلاً للمصادقة. ويجب على مسؤول النظام فتح الحساب للمستخدم لاستعادة الوصول للنظام.
- إقفال كلمة السر المحلية - إذا تم تمكين هذه الخاصية فإن المستخدم لن يتمكن من إتمام عملية المصادقة بكلمة السر الموجودة في (/etc/passwd). لكن المصادقة الخارجية باستخدام البروتوكول الخفيف للوصول للدليل (LDAP)، وبروتوكول المصادقة على شبكات الكمبيوتر (Kerberos)، وخدمة معلومات الشبكة (NIS) وغيرها لا يزال مسموحاً.
- انتهاء صلاحية كلمة المرور- ضبط الحد الأدنى والحد الأقصى من الوقت الذي يمكن أن يمر بين فترات تغيير كلمات المرور. وعند انقضاء الحد الأقصى للوقت يقوم مسؤول النظام بفتح الحساب حتى يتمكن المستخدم من الوصول للنظام.

الشكل (٣-٥): الوصول لمدير المستخدمين والمجموعات



الشكل (٣-٦): إضافة مستخدم



الشكل (٣-٧): مدير المجموعة



- التغيير الإلزامي لكلمة المرور عند تسـجيل الدخول القادم - والمعنى هنا واضح ولا يحتاج إلى تفسـير. ويُسـتخدم هذا الإعداد في كثير من الأحيان للحسابات الجديدة حيث يقوم مسـؤول النظام بإنشـاء حسـاب جديد بكلمة سر بسـيطة ومعروفة. وعندما يقوم المستخدم بتسـجيل الدخول للمرة الأولى فإنه يُطلب منه تغيير كلمة المرور إلى أخرى أكثر أمناً.

وبالإضافة إلى المســتخدمين فإن علامة تبويب المجموعات (groups) تسمح بإدارة كل ما يخص المجموعة كالإنشــاء والحذف وتغيير العضوية (الشــكل ٣-٧). ولإضافة مجموعة جديــدة اختر زر إضافة مجموعــة (Add Group)، وأدخِل اســماً للمجموعــة الجديدة. وبإمكانك أيضاً تحديد رقم تعريف مخصص للمجموعة إنْ لزم الأمر. وعند إنشاء المجموعة سيتســنى لك إضافة أعضاء لها. اختر اسم المجموعة من القائمة الموجودة في علامة تبويب المجموعات وانقر على زر خصائص (Properties). وعندها ســيتم عرض النافذة الموضحة على يمين الشــكل. وعليك أن تنقر على مربع الاختيار الموجود بجوار كل مســتخدم ترغب بإضافتــه كعضــو، وبعد ذلك انقر فــوق موافق (OK). الآن مجموعتــك الجديدة جاهزة للاستخدام.

إدارة مُستخدم سطر الأوامر (Command-line user administration):

من الســهل جداً اســتخدام الواجهة الرسومية لـ (إدارة المســتخدم) حيث يمكن عملياً استخدامها لجميع مهام إدارة المستخدم، لكن ما الذي يمكن أن تفعله إذا كانت حزمة إدارة المســتخدم غــير متوفرة أو كنت تعمل على نظام عن بعد عــبر اتصال الطلب الهاتفي؟ في مثل هذه الحالات فإن (واجهة سطر الأوامر) هي الخيار الأفضل. والخبر السار هو أن لكل شيء في نظام ينكس مكافئاً في ســطر الأوامر. في الواقع فإن العديد من الأدوات الرســومية في نظام ينكس مجرد واجهات أمامية تقوم بجمع البيانات من المســتخدم، وتشغيل برنامج سطر الأوامر، وعرض النتائج.

ويمكن اســتخدام الأوامر (useradd) و (usermod) و (userdel) لإدارة معظم المهام الموجودة في إدارة المستخدم. ومثل العديد من الأوامر الأخرى التي ناقشناها في هذا الفصل فإن هذه الأوامر لها قدرات مختلفة اعتماداً على نظام التشغيل الذي تعمل عليه. وتحتوي الإصدارات الموجودة مع نظام ســينتوس على بعض الميزات المتقدمة التي يمكننا الاســتفادة منها، ولكن سوف نكتفي بتوضيح المواصفات المتوفرة في المنصات المتعددة.

وفي هذا المثال ســوف نقوم بإنشاء مستخدم جديد بحيث يكون اسم المستخدم (fred) والدليل الرئيسي (-home/fred/) (d). كما ســنقوم أيضاً بحفظ الاسم الكامل للمستخدم في حقل ملاحظات ملف كلمة المرور (-Fred Flintstone «c»).

```
[root@sunshine ~]# useradd -c "Fred Flintstone" -m -d "/home/fred" fred
[root@sunshine ~]# ls -laF /home/fred
total 28
drwx------.  4 fred fred 4096 May  4 19:48 .
drwxr-xr-x.  9 root root 4096 May  4 19:48 ../
-rw-r--r--.  1 fred fred   18 May 10  2012 .bash_logout
-rw-r--r--.  1 fred fred  176 May 10  2012 .bash_profile
-rw-r--r--.  1 fred fred  124 May 10  2012 .bashrc
drwxr-xr-x.  2 fred fred 4096 Nov 11  2010 .gnome2/
drwxr-xr-x.  4 fred fred 4096 Jan 22 18:48 .mozilla/
```

وقبل أن يتمكن المستخدم الجديد من الدخول على حسابه سنحتاج إلى ضبط كلمة المرور. وعندما تقوم باستخدام أمر (useradd) فإنه يترك حقل كلمة السر فارغاً مما يؤمن الحساب بشكل فعّال حتى يتم تعيين كلمة المرور. أما أمر (passwd) فإنه يسمح لك بضبط كلمة المرور في الحساب المصرح لك القيام بذلك. وبينما يوضح المثال التالي كلمة السر فإنه عملياً ولأسباب أمنية لا يتم عرض كلمة السر. وبما أنك على الأرجح ستحتاج إلى كتابة كلمة السر (على ورقة أو في البريد الإلكتروني أو في ملف ما) لإعطائها للمستخدم الجديد، يتوجب عليك أن تطلب من المستخدم تغيير كلمة السر عند أول تسجيل دخول. وستقوم بعمل ذلك في سينتوس باستخدام المفتاح (e-) مع الأمر (passwd):

```
[root@sunshine ~]# passwd fred
Changing password for user fred.
New password:  NewPasswordGoesHere
Retype new password:  NewPasswordGoesHere
```

```
passwd:  all authentication tokens updated successfully.
[root@sunshine ~]# passwd -e fred
Expiring password for user fred.
```

الآن بإمكان المستخدم (fred) تسجيل الدخول على النظام والوصول لملفاته. وبالإضافة إلى مفتاح (-e) فإن هناك العديد من المفاتيح المفيدة في التحكم بالوصول التي يســمح بها الأمر (passwd) مثل إقفال حســاب (-l) وفتح حســاب (-u) وضبــط العمر الأدنى لكلمة المرور (-n) وكذلك ضبط العمر الأقصى لكلمة المرور (-x).

```
[root@sunshine ~]# passwd -l fred
Locking password for user fred.
[root@sunshine ~]# passwd -u fred
Unlocking password for user fred.
[root@sunshine ~]# passwd -n 1 -x 180 fred
Adjusting aging data for user fred.
```

ولإضافة المســتخدم كعضو في مجموعة موجودة بإمكانك اســتخدام الأمر (usermod) مع مفتاح (-aG)، ويتوجب عندها فصل أسماء المجموعات بفاصلة.

```
[root@sunshine ~]# groups fred
fred :  fred
[root@sunshine ~]# usermod -a -G
coll_fine_arts_grp,vp_academic_aff_grp fred
[root@sunshine ~]# groups fred
fred:  fred vp_academic_aff_grp coll_fine_arts_grp
```

وبإمكانك أيضاً اســتخدام الأمر (usermod) لتعديل بعض من خيارات الحســاب مثل تاريخ الانتهاء (e-) ونقل الدليل الرئيسي (md-).

```
[root@sunshine ~]# usermod -e 201301-08- -md "/home/flintstone" fred
[root@sunshine ~]# ls -laF /home/flintstone
total 28
drwx------.  4 fred fred 4096 May  4 19:48 .
drwxr-xr-x.  9 root root 4096 May  4 19:48 ../
-rw-r--r--.  1 fred fred   18 May 10  2012 .bash_logout
-rw-r--r--.  1 fred fred  176 May 10  2012 .bash_profile
-rw-r--r--.  1 fred fred  124 May 10  2012 .bashrc
drwxr-xr-x.  2 fred fred 4096 Nov 11  2010 .gnome2/
drwxr-xr-x.  4 fred fred 4096 Jan 22 18:48 .mozilla/
```

وأخيراً فإن الأمر (userdel) يقوم بحذف حســاب المســتخدم. وافتراضيــاً لا تتم إزالة الدليل الرئيسي لحساب المستخدم ولإزالته يتوجب إضافة المفتاح (r-).

```
[root@sunshine ~]# userdel -r fred
[root@sunshine ~]# ls -laF /home/flintstone
ls:  cannot access /home/flintsone:  No such file or directory
[root@sunshine ~]# groups fred
groups:  fred:  No such user
```

إدارة المجموعة:

وبشـــكل مشـــابه لأوامر إدارة المســـتخدم (useradd) و(usermod) و(userdel) فإن هنـــاك أوامر مطابقة لهـــا وموجهة لإدارة المجموعة وهـــي (groupadd) و(groupmod) و(groupdel). ولأن المجموعـــات لديها عدد قليل جداً مـــن الخيارات القابلة للضبط فإن لهـــذه الأوامر عـــدداً قليلاً جداً من المفاتيح المســـتخدمة. ولا يحتاج الأمـــران (useradd) و(userdel) إلى أي معايير إضافية ســـوى أن تقـــوم المجموعة بالعمل، والخيار الوحيد لأمر (usermod) هو إعادة تســـمية المجموعة باستخدام (n-). ويمكن إدارة عضوية المجموعة باســـتخدام الأمـــر (groupmems) والذي يتضمن مفتاح للإضافـــة (a-)، وآخر للإزالة (d-) وثالث لسرد جميع أعضاء المجموعة (l-).

```
[root@sunshine ~]# groupadd new_group
[root@sunshine ~]# groupmems -a alice -g new_group
[root@sunshine ~]# groupmems -a bob -g new_group
[root@sunshine ~]# groupmems -l -g new_group
alice  bob
[root@sunshine ~]# man groupmod
[root@sunshine ~]# groupmod -n improved_group new_group
[root@sunshine ~]# groupmems -l -g improved_group
alice  bob
[root@sunshine ~]# groupmems -l -g new_group
groupmems:  group ‘new_group’ does not exist in /etc/group
[root@sunshine ~]# groupdel improved_group
```

نموذج حالة - كلية شمال غرب ولاية فلوريدا (Northwest Florida State College):

في شـــهر أكتوبر من عام ٢٠١٢ تم إعلان سرقة المعلومات الشخصية لأكثر من ٣٠٠ ألف شخص من كلية شمال غرب ولاية فلوريدا. وتخدم الكلية، التي كانت سابقاً كلية مجتمع، نحو ١٧ ألف طالب ســنوياً. ومنذ تأسيســها في عام ١٩٦٣ منحت الكلية ما يُقارب ٣٠ ألف درجة علمية[١٣].

وبلغ عدد المتضررين ما يقارب ٢٠٠ ألف شخص من الذين ليس لهم علاقة بالكلية. كما شــمل الضرر أيضاً أكثر من ٧٥ ألفاً من الطلاب الســابقين والحاليين، وكذلك ٣٢٠٠ موظف حالي أو متقاعد. وبالنسبة للمتضررين غير المنتسبين للكلية والذين بلغ عددهم ٢٠٠ ألف شــخص هم من الطلاب المؤهلين للحصول على المنح الدراســية التابعة لبرنامج المســتقبل المــشرق (Bright Futures) في الســنوات الدراســية التــي تبدأ في عامــي ٢٠٠٥ و ٢٠٠٦ . وتضمنــت البيانات المسروقة الأســماء وأرقام الضمان الاجتماعــي وتواريخ الميلاد والجنس والعرق. أما بالنســبة للموظفين فقد اشتملت البيانات المسروقة على أرقام حسابات إيداع الرواتــب. وفي وقت إعلان هذه الحادثة اعترفت الجامعة بأن ما يقارب من ٥٠ موظفاً، بما في ذلك رئيس الجامعة، قد أبلغوا عن قضايا متضمنة لسرقة الهوية.

واســتناداً إلى تحقيقات الكلية، والتي أُجريت بمســاعدة خبير استشــاري خارجي وكذلــك بمســاعدة خبير جرائم الإنترنــت في مكتب نقيب شرطة مقاطعة أوكولوســا (Okaloosa County Sheriff's Office)، أن الاختراق حدث ما بين ٢١ من شهر مايو و٢٤ من شــهر ســبتمبر من عام ٢٠١٢. وتتوقع الكلية أن الاختراق «احترافي ومنســق حدث من قرصان واحد أو أكثر».

وشــمل الاختراق مجلد من الخادم الرئيسي للكلية يحتوي على عدة ملفات. وفي حين أن الكليــة أمّنت الملفات بحيــث لا يوجد ملف واحد يحتوي على كامل المعلومات الشــخصية المتعلقة بالأفراد، لكن في حال تمكن القراصنة من الوصول إلى خادم واحد يحتوي على الملفات فإنهم سيكونون قادرين على تجميع كل المعلومات المطلوبة عن ٥٠ موظفاً على الأقل.

(١٣) وذلك حسب الإصدار الأخير من كتيب الحقائق الخاص بالكلية في وقت كتابة هذه السطور (٢٠١٠-٢٠١١).

واســتخدم المهاجمون الهويات المسروقة للحصول على (قروض على الراتب) من شركتين في كندا وهــما: شركة (.PayDayMax, Inc) وشركة (Discount Advance Loans (iGotit.com, Inc.)) . كما استخدموا أوراق الاعتماد البنكية المسروقة لسداد تلك القروض. وبالإضافة إلى ذلك تم اســتخدام البيانات المسروقة للحصول على بطاقــات ائتمانية من شركة هوم ديبو (Home Depot) بأسماء موظفي الكلية.

المراجع:

Ragan, S. “Northwest Florida State College says clever attackers were successful in data breach,” SecurityWeek, October 10, 2012.

Bolkan, J. “Northwest Florida State College data breach compromises 300,000 students and employees,” Campus Technology, October 17, 2012.

الملخص:

يوضح هذا الفصل العديد من الأدوات الأساســية التي يســتخدمها مســؤولي الأنظمة. وتُعــد المعرفة المعقولة بهذه الأدوات شرطاً أساســياً لتحقيق النجــاح المهني في مجال أمن المعلومات. ويقدم هذا الفصل أمثلة ملموســة على مهام إدارة الأنظمة التي نوقشــت في الفصل الســابق. والهدف من هــذا الفصل تحقيق فهم جيد لكل مــن إدارة نظام ينكس بشــكل عام وتوزيع سينتوس لينكس بشكل خاص. وهذه المعرفة ستكون أساساً للنقاشات التقنية التي سنتعرض لها في بقية هذا المقرر الدراسي.

أسئلة مراجعة للفصل:

١. ما وظيفة نواة نظام التشغيل (kernel)؟

٢. مــا القشرة (shell)؟ ما برنامج القشرة الموجود في جميع إصدارات نظام ينكس؟ وما موجه القشرة (shell prompt)؟

٣. ماذا يُطلق على قمة هرم هيكلة نظام الملفات؟ وكيف يتم عرضها في أنظمة ينكس؟

٤. ما المسار؟ وما الفرق بين المسار النسبي والمسار المطلق؟

٥. فيمَ يُســتخدم أمر نظام ينكس (pwd)؟ وما هــي بعض الخيارات المفيدة التي تأتي مع هذا الأمر؟

٦. فيمَ يُســتخدم أمر نظام ينكس (cd)؟ وما هي بعض الخيارات المفيدة التي تأتي مع هذا الأمر؟

٧. فيمَ يُســتخدم أمر نظام ينكس (ls)؟ وما هي بعض الخيارات المفيدة التي تأتي مع هذا الأمر؟

٨. فيمَ يُستخدم أمر نظام ينكس (rm)؟ وما هي بعض الخيارات المفيدة التي تأتي مع هذا الأمر؟

٩. فيمَ يُستخدم أمر نظام ينكس (mkdir)؟ وما هي بعض الخيارات المفيدة التي تأتي مع هذا الأمر؟

١٠. اذكر أمرين من الأوامر التي يمكنك استخدامها في تغيير الدليل الرئيسي.

١١.ما امتداد اسم الملف (wildcards)؟ واذكر مثالاً يوضح كيفية استخدام واحد منها؟

١٢.ما التكرارية في سياق عمليات الملف؟ وكيف تكون مفيدة؟ ولماذا يتوجب أن تكون حذراً على الخصوص عند استخدامك للتكرارية في أوامر الملف؟

١٣.ما الطريقة المفيدة لاستخدام أمر (tail) لعرض ملفات السجل (log files)؟

١٤.كيف يمكنك اســتخدام أمر (find) للبحث عن مجلد الرســائل (messages) والذي تعلم عن وجوده في مجلد (/var)؟

١٥.بالنظــر إلى مخرجات أمر (ls –l) الموجودة أدناه، مــا الذي تعرفه عن ملكية مجلد (accounting) وعن أذونات الوصول إلى هذا المجلد؟

drwxr-xr-x. 2 root accounting_grp

4096 Jan 28 19:07 accounting/

١٦.وبالنظــر إلى مخرجــات أمر (ls) أعلاه، كيف يمكنك اســتخدام أمــر (chmod) لإعطاء أذونات الكتابة لجميع أعضاء مجموعة (accounting_grp) في مجلد (accounting)؟

١٧.ما قوائم التحكم في الوصول؟ وكيف يتم استخدامها؟

١٨.يُستخدم الأمر (setfacl)؟

١٩.يُستخدم الأمر (getfacl)؟

٢٠.لماذا المعرفة العملية بمحرر (في-آي) مهمة بالنسبة لمسؤولي تقنية المعلومات؟

٢١.وضح كيف يتصرف الملف التنفيذي (setuid) عند تشغيله.

٢٢.ما الذي على مالك ملف (.bashrc) أن يقوم به ليتمكن من تحرير الملف إذا كانت أذوناته الحالية هي ٤٤٤؟

٢٣.ما حزمة البرمجيات؟ ما الأشكال الشائعة في توزيع حزم البرمجيات؟

٢٤.كيف يمكنك البحث عن جميع حزم البرمجيات المثبتة في نظامك؟

٢٥.كيف تستخدم الأمر (yum) لتحديث جميع البرمجيات في النظام؟

أسئلة على نموذج الحالة:

١. أبقت الكلية على رابط صفحة إلكترونية على صفحتها الرئيسية (http://www.nwfsc.edu/)[(١٤)] وذلك لتوضيح تفاصيل استجابة الكلية المستمرة للاختراق. بناءً على تلك المعلومات، ما الحقائق التي يمكنك إضافتها إلى تفاصيل الحالة الموضحة هنا؟

٢. إذا تم اختراق هويتك، ما الضرر الذي يمكن أن يحدث لحياتك الشخصية؟

٣. ما توصيات لجنة التجارة الاتحادية (FTC) بشأن الخطوات التي يجب اتباعها في حال اختراق المعلومات الشخصية الخاصة بك؟

٤. في رأيك ما الخطوات الثلاث الأكثر أهمية التي يمكن اتخاذها لمنع سرقة الهوية في المقام الأول؟

---

(١٤) التحقق الأخير تم في تاريخ ٢٠١٣/٢٢/٠٢

نشاط التدريب العملي-الإدارة الأساسية لنظام لينكس:

تهدف هذه الأنشـطة لإظهار معرفتك بالأوامر التي تعلمتها في هذا الفصل. باستخدام الآلة الافتراضية لنظام لينكس التي أنشأتها في الفصل الثاني، افتح نافذة طرفية باختيار لوحة أدوات النظـام (System Tools) ضمن قائمة تطبيقات (Applications). بعد الانتهاء من كل تمرين قم بتسليم النتائج المطلوبة إلى أستاذ المادة.

تمرين ١:

١,١ غير الأدلة إلى (/opt/book/system-admin).

١,٢ اذكر جميع محتويات الدليل (متضمناً ذلك المحتويات المخفية).

النتيجة المطلوب تسليمها: خذ صورة من الشاشة لمحتويات الدليل.

تمرين ٢:

غير الأدلة إلى (/opt/book/system-admin/ex٢).

أعد تسمية الملف (jeklyll.txt) إلى (hyde.txt).

أنشئ نسخة لملف (prince.txt) باسم (pauper.txt).

احذف الدليل التالي وجميع محتوياته (Jacob.marley).

النتيجة المطلوب تسليمها: خذ صورة من الشاشة لمحتويات الدليل.

تمرين ٣:

جِد الملف المُسمى بـ (gettysburg.txt).

اعرض آخر ثلاثة سطور من نص ملف (gettysburg.txt).

جِد الملف المُسمى بـ (declaration.txt).

اعرض آخر خمسة سطور من نص ملف (declaration.txt).

النتيجة المطلوب تسـليمها: خذ صورة من الشاشـة تحتوي على السطور المطلوبة من ملف (gettysburg.txt) ومن ملف (declaration.txt).

تمرين ٤:

أنشئ ثلاثة مستخدمين جدد:

الاسم: Thomas Jefferson.

اسم المستخدم: thomas.

كلمة السر: Monticello.

الاسم: Abraham Lincoln.

اسم المستخدم: abe.

كلمة السر: ٧years&٤score.

الاسم: Benjamin Franklin.

اسم المستخدم: ben.

كلمة السر: Early2bedEarly2rise.

أنشئ ثلاث مجموعات جديدة:

Presidents (الأعضاء: thomas, abe).

continental_congress (الأعضاء: thomas, ben).

us_currency (الأعضاء: thomas, ben, abe).

اجعل (thomas) مالكاً للملف (declaration.txt) من التمرين السابق.

اجعل (abe) مالكاً للملف (gettysburg.txt) من التمرين السابق.

غير ملكية المجموعة لملف (declaration.txt) إلى مجموعة (continental_congress) واجعــل الملف قابلاً للكتابة من قبــل المجموعة. يُفترض أيضاً أن يكون الملف قابلاً للقراءة من جميع الأعضاء.

النتيجة المطلوب تســليمها: خذ صورة من الشاشة لأذونات وصول الأفراد/ المجموعات للملفين المذكورين.

تمرين ٥:

قــم بتثبيت حزمــة (apps-xorg-x١١) وهي مجموعة من الأدوات الشــائعة لواجهة المستخدم الرسومية (GUI).

قم بتشغيل الأمر (xclock).

افتح نافذة طرفية جديدة وقم بتشغيل الأمر (apps-yum list xorg-x١١).

النتيجة المطلوب تسليمها: خذ صورة من الشاشة للنافذة الطرفية ولنافذة (xclock).

تمرين ٦:

قم بتحديث حزم الـ (RPM) المُثبتة حالياً في النظام.

النتيجة المطلوب تسليمها: خذ صورة من الشاشة للسطر الأول من (/etc/issue).

تمرين التفكير النقدي-عمليات التأثير الإلكتروني الهجومية (OCEO):

من بين الوثائق التي نشرها إدوارد سنودن، وهو المتعهد الذي كان يعمل في وكالة الأمن القومي الأمريكية (NSA)، بعد استقالته من الوكالة وثيقة توجيهات السياسة الرئاسية رقم ٢٠ (PPD20) الصادرة في أكتوبر من عام ٢٠١٢. وضمن أشــياء أخرى، وردت مذكرة سرية للغايــة تتكون من ١٨ صفحة قامــت بتحديد دور (عمليات التأثــير الإلكتروني الهجومية-OCEO) والتــي تم تعريفها بأنها "العمليات والبرامج ذات الصلة أو الأنشــطة الشــاملة لدفاع الشبكة، والمجموعة السيبرانية، أو (DCEO)-التي أُجريت بواسطة حكومة الولايات

المتحـدة الأمريكيــة أو نيابة عنها، في الإنترنــت أو من خلالها، بهدف تمكــين أو إنتاج آثار الإنترنت خارج شبكات الحكومة الأمريكية".

وينص وصف (عمليات التأثير الإلكتروني الهجومية) في وثيقة (PPD20) على ما يلي:

ويمكــن أن تقدم (عمليات التأثير الإلكتروني الهجومية) قدرات غير تقليدية وفريدة من نوعهــا لتحقيق أهــداف الولايات المتحدة القومية في جميع أنحــاء العالم بتحذير ضئيل أو معدوم للعدو أو الهــدف، وبتأثير يتراوح بين إحداث إضرار غير ملحوظة إلى إحداث أضرار كبيرة. لكن تطوير واستدامة قدرات (عمليات التأثير الإلكتروني الهجومية) قد تتطلب وقتاً وجهداً كبيراً إذا لم يكن الوصول والأدوات لهدف محدد موجود بالفعل.

ويتعــين على حكومة الولايات المتحدة تحديد أهداف ممكنة ذات أهمية وطنية حيث تكون (عمليات التأثير الإلكتروني الهجومية) قادرة على تقديم توازن مناســب من الفعالية والمخاطرة مقارنةً بغيرها من أدوات الســلطة الوطنية، وإنشــاء قدرات لـ (عمليات التأثير الإلكــتروني الهجوميــة) والحفاظ عليها، وتكــون تلك القدرات متكاملة حســب المُلائم مع القــدرات الهجومية الأمريكية الأخرى، وتنفيــذ تلك القدرات بطريقة تتفق مع أحكام هذا التوجيه.

أنت تدخل في عالم محترف يعمل في هذه البيئة.

المراجع:

Bruce Schneier's Cryptogram, July 15, 2013

Schneier, B. "Has U.S. started an Internet war?", CNN, 2013, http://www.cnn.com/201318/06//opinion/schneier-cyberwar-policy (accessed 072013/16/)

The Guardian, "Obama tells intelligence chiefs to draw up cyber target list – full document text", 2013.

أسئلة على تمرين التفكير النقدي:

١. بعبارات واضحة ما هي (عمليات التأثير الإلكتروني الهجومية)؟

٢. ما هي بعض الأنشطة التي قد تُشكل (عمليات التأثير الإلكتروني الهجومية)؟

٣. مـا هي بعض التداعيات لخبراء أمـن المعلومات الذين يعملون في الولايات المتحدة الأمريكيـة (وربما أيضاً خـارج الولايات المتحدة) بعد أن أصبـح الكل مدركاً لوثيقة (PPD20)؟

تصميم حالة:

تمت دعوتك لإلقاء نظرة على محطة عمل البروفسور التي تعمل بنظام لينكس. الجهاز جديـد كلياً ويحتوي عـلى معالج سريع وذاكرة كبيرة، لكن منذ نحو أسـبوع أصبح الجهاز بطيئاً للغاية.

أول الأشياء التي عليك معرفتها عند النظر في مشكلات الأداء في نظام ينكس هو تشغيل الأمـر (ps) والذي يرمز إلى وضـع المعالـج (processor status). وتوضح مخرجات هذا الأمر جميع العمليات التي هي قيد التشغيل في محطة العمل، كما توضح بعض المعلومات الإضافية عن حالة تلك العمليات.

كـما توضح مخرجات الأمر (ps) جميع عمليات نظام التشـغيل العادية التي تتوقع أن تراها تعمل في النظام، لكنك سترى أيضاً بعض العمليات التي تبدو خارجة عن المألوف:

- /home/taylor/.sh يعمل كجذر.
- /home/taylor/…/ncftpd, يسـتهلك الكثـير مـن مخرجـات ومدخلات وحدة المعالجة المركزية والقرص.

الدليـل (/home/taylor) هو الدليل الرئيسي للبروفيسـور الدكتور تايلور. وهنا بعض المعلومات الإضافية التي قمت بجمعها خلال الفحص:

- تم ضبط الأذونات في دليل (/home/taylor/.sh) إلى ٧٥٥١.
- ملكية الملف تعود للجذر.
- (hash MD٥) مطابق لـ (/bin/bash) مما يعني أن الملفات هي نفسها تماماً.
- يحتوي الدليل (/home/taylor/...) على ملفين:

ملف (ncftpd) والذي وجدته يعمل سابقاً بأمر (ps).

ملف (general.cf) ويملكه تايلور وأذوناته ٦٤٤.

ملف (domain.cf) ويملكه تايلور وأذوناته ٦٤٤.

- هذا الملف (general.cf) يتضمن من بين الأسطر الأخرى ما يلي:

log-xfers= yes

port = 80

- الملــف التالي (domain.cf) أرشــدك إلى ملف ســجل. وهذه هــي مخرجات أمر (head -٧) من ملف السجل:

201223:30:59 20-04- ### | S,/var/tmp/pub/

StarWars.avi, ...

201223:35:59 20-04- ### | S,/var/tmp/pub/

Conan.avi, ...

201223:37:59 20-04- ### | S,/var/tmp/pub/

Avatar.avi, ...

201200:37:59 21-04- ### | R,/var/tmp/pub/

Avatar.avi, ...

201200:37:59 21-04- ### | R,/var/tmp/pub/

Avatar.avi, ...

201201:37:59 21-04- ### | R,/var/tmp/pub/

Avatar.avi, ...

201202:35:59 21-04- ### | R,/var/tmp/pub/

Conan.avi, ...

اكتب تقريراً عن المشــكلة التي تعتقد بوجودها في محطة العمل واقترح خطوات لحل المشكلة استناداً إلى ما تعرفه.

أسئلة إرشادية:

جهاز الحاسب مُخترق بالتأكيد. ويدعي الدكتور تايلور أنه ليس لديه فكرة عمن وضع البرامج في جهازه. وهناك موضوعان مختلفان بناءً على ما وجدت: الموضوع الأول يؤثر في أداء الجهــاز، والموضوع الثاني أكــثر خطورة ويؤثر في توصيتك النهائية حيال ما يجب القيام به مع جهاز الحاسب.

- ناقش برنامج (sh) والذي وجدته في الدليل الرئيسي.
- ما الذي يحدث عند تشغيل مستخدم "عادي" مثل تايلور لهذا البرنامج.
- هل باستطاعة المستخدم، الذي ليس لديه صلاحية مسؤول النظام، أن يقوم بتغيير الملف إلى جذر؟
- هل باستطاعة المستخدم، الذي ليس لديه صلاحية مسؤول النظام، أن يقوم بإضافة مالك (setuid)؟
- ماذا يمكن أن يقال عن المستخدم الذي وضع الملف هناك في المقام الأول؟
- ما هو برنامج (ncftpd)؟ قم ببعض البحث على الإنترنت إن كان ذلك ضرورياً.

- في رأيك ما هو الغرض من هذا البرنامج؟
- هل لديك تخمين مدروس بخصوص متى تم تثبيت البرنامج أو متى بدأ في عملياته؟
- بناءً على ما تعرفه، ما الذي يجب عمله بمحطة العمل؟ ولماذا؟

أسئلة إضافية:

- ماذا يعني سطر المنفذ ٨٠ في ملف الضبط؟
- ولماذا تم ضبطه بهذه الطريقة؟



الفصل الرابع

النموذج الأساسي لأمن المعلومات

من المسؤول عن الأمن على شبكة الإنترنت؟ وكيف أعرف ذلك؟

(كتاب: Cuckoo's Egg)

نظرة عامة:

يقدم هذا الفصل النموذج الأســاسي المُستخدم في تطبيق أمن المعلومات والذي يتكون من أربعة عناصر: الأصول، والثغرات الأمنية، والتهديدات، والضوابط. وسوف نُعرّف هذه المصطلحــات، ونقــدم أمثلة لكل منها، ونوضح كيفية ارتبــاط بعضها ببعض. في نهاية هذا الفصل يجب أن تعرف:

- عناصر النموذج الأساسي لأمن المعلومات.
- العلاقة بين عناصر النموذج الأساسي لأمن المعلومات.
- التصنيف الشائع لضوابط أمن المعلومات.

مقدمة:

ســلّطت الفصول السابقة الضوء على أهمية أمن المعلومات. وفي مُعظم المنظمات يقع الجزء الأكبر من مســؤولية الحفاظ على أمن المعلومات على عاتق مســؤولي الأنظمة. ومن أجل زيادة اهتمامك بأمن المعلومات عرضت الفصول السابقة المهام الأساسية التي يقوم بها مسؤولو الأنظمة والمهارات المطلوبة منهم لإتمام هذه المهام. وفي الفصول اللاحقة سنواصل تعزيز هذه المهارات التقنية.

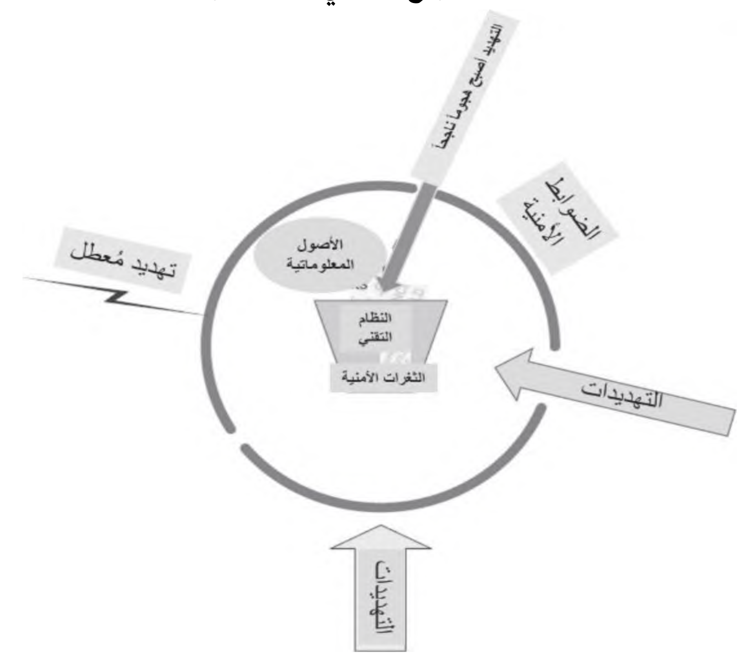
ويُعد موضوع أمن المعلومات موضوعاً متشــعباً لأن معظم حوادث أمن المعلومات تتم مــن خلال اســتغلال الثغرات الأمنية الجديدة في المنظمة. ومــن ثم فإن الحفاظ على أمن

المعلومــات يتطلب الانتباه إلى جميع جوانــب المنظمة. ولتوفير هيكلة لهذه الجهود، فإنه من المفيد تنظيم جميع الأنشــطة المرتبطة بالحفاظ على أمن المعلومات في إطار أو نموذج. وفي هذا الكتاب نســمي هذا النموذج بالنموذج الأســاسي لأمن المعلومات وهو موضح في الشكل (٤-١).

مكونات النموذج الأساسي لأمن المعلومات:

النموذج هو تمثيل للعالم الحقيقي. وتكون النماذج مفيدة في لفت الانتباه إلى العناصر الأساسية للمشكلة. ويشتمل نموذج أمن المعلومات على المكونات الأساسية لأمن المعلومات، ويوضــح علاقة هذه المكونات بعضها مع بعض، ويســتبعد النموذج أي شيء آخر. ويظهر النموذج الأســاسي لأمن المعلومات المســتخدم في هذا الكتاب في الشــكل (٤-١). ويتكون النموذج من أربعة عناصر: (١) الأصول، (٢) الثغرات الأمنية، (٣) التهديدات، (٤) الضوابط. وكل نشاط يتعلق بأمن المعلومات يقع تحت أحد هذه العناصر.

الشكل (٤-١): النموذج الأساسي لأمن المعلومات



الأصول:

تأتي الأصول في وسـط الشـكل (٤-١). وفي سـياق أمن المعلومات، تُعرف الأصول بأنها الموارد أو المعلومات التي نسعى للحفاظ عليها. وفي جميع الحالات الأمنية، سواء تلك التي تتعلق بأمن المعلومات أم بأمن المنزل الشخصي، تبدأ تلك الحالات بالأصول التي تُعد ثمينة بما فيه الكفاية بالنسـبة لك لبذل جهد خاص للحفـاظ عليها من الضرر. وأمن المعلومات لا يختلـف عن ذلك. فإذا كانت المعلومات أو الموارد ذات الصلة ثمينة بالنسـبة للمنظمة، عندها تحتاج المنظمة لبذل جهد خاص لتأمين المعلومات.

ومـع ذلك هناك اختلافان مُهمان بين الأصول التقليدية وأصول المعلومات وهما: تعذر الرؤيـة، وقابلية التكرار. ففـي معظم الحالات الأمنية التي أنت عـلى علم بها فإنه يمكن رؤيـة العنـاصر التي يتعين حمايتها. على سـبيل المثال تقوم بقفل سـيارتك لحمياتها من السرقة، وتركب أنظمة إنذار لمنع إقتحام منزلك. وفي كلتا الحالتين فإن الأصول مرئية بالعين المُجردة، والضرر واضح أيضاً، فإذا اقتحم شـخص سيارتك أو منزلك فإن الضرر يكون واضحاً على الفور. وإذا كان بالجوار كاميرات مراقبة فإنها سـتلتقط التخريب المُتعمد الذي حدث للممتلكات.

لكن أمن المعلومات مختلف. فالأصول في مجال أمن المعلومات ليست أدوات ملموسة يمكن رؤيتها وتحسسـها. وبدلاً من ذلك فإن الأصول في مجال أمن المعلومات هي البيانات والمعلومات المخزنة بشكل أصفار (٠s) وآحاد (١s) في أجهزة الكمبيوتر والأشرطة والهواتف والأجهـزة المختلفـة. وفي حين يمكن رؤية الأقراص الصلبة والأجهـزة الأخرى، فإنه لا يمكن رؤية البيانات الثمينة المُخزنة في تلك الأجهزة. وإذا تمت سرقة البيانات عبر الشبكة فإنه لا يمكن رصد عملية نقل البيانات عبر الكاميرات والأجهزة الأمنية التقليدية. ويعمل اللصوص عادة من دولة مختلفة على بُعد آلاف الأميال في مأمن من مراقبة وكالات الأمن التقليدية.

الفـرق المهـم الآخر بـين الأصول التقليديـة وأصول المعلومـات هو القابليـة للتكرار. واستكمالاً لمثال السيارة السابق، فإن السيارة إذا سُرقت فإنك ستلاحظ في الصباح أن السيارة مفقودة، وذلك لأن السـيارة يمكن أن توجـد في مكان واحد فقط في أي وقت من الأوقات، وعـلى النقيض من ذلك فإن المعلومات يمكن تكرارها بإتقان. إذا تمت سرقت بيانات فإنك

لن تلاحظ عملية السرقة ما لم يقم أحد ما بلفت نظرك للحادثة. على سبيل المثال، إذا لاحظ شخص ما أن جهاز الكمبيوتر المحمول الخاص بك دون رقابة فقام بإرسال نسخة من واجبك المنزلي إلى بريده الإلكتروني، وبعد ذلك قام بتسليم الواجب على أنه عمله الشخصي. ففي هذه الحالة لن يكون لديك أدنى فكرة عن عملية الانتحال هذه وخصوصاً إذا لم يقم أستاذ المادة بلفت نظركم إليها.

هذان الفرقان بين الأصول التقليدية وأصول المعلومات - تعذر الرؤية، وقابلية التكرار - تجعل من أمن المعلومات تحدياً مختلفاً إلى حد كبير عن الأمن التقليدي. فالأساليب الأمنية التقليدية مثل الأقفال والحراس ليست فعالة في الحفاظ على أمن المعلومات. على سبيل المثال، لن تقوم الأقفال التقليدية بفعل شيء يُذكر لمنع سرقة البيانات عبر الشبكة. فالأصول التقليدية المسروقة كالذهب يمكن استردادها وإعادتها إلى أصحابها. لكن البيانات المسروقة يمكن نسخها إلى مائة موقع، وحتى لو تم تدمير بعض هذه النسخ، فإنه يكاد يكون من المستحيل أن نُنكر استفادة اللص من وصوله إلى البيانات. ومن ثم يتعين على ضوابط أمن المعلومات محاولة منع السرقة في المقام الأول، وكشف السرقات ومنعها عند حدوثها من خلال المراقبة المستمرة.

ولقرون عدة كان الذهب مقياساً موحداً لقيمة الأشياء. ووفقاً لذلك، وللدلالة على قيمة المعلومات، فإن الأصول المعلوماتية في النموذج الأساسي (الشكل ٤-١) تظهر على هيئة سبائك ذهبية (المعلومات التي في حوزة العديد من المنظمات قد تكون قيمتها في الواقع أعلى من الذهب!).

> الحالة الأكثر شيوعاً التي ستواجهها هي أن يتم حفظ أصول المعلومات في نظام تقنية المعلومات. النظام الورقي لا يستطيع أن يُلبي متطلبات المنظمات الحديثة من حيث المساحة الكبيرة لحفظ المعلومات. ويُعرف نظام تقنية المعلومات بأنه مجموعة من مكونات أجهزة الحاسب الآلي والبرمجيات والبرامج الثابتة المهيأة لغرض معالجة وتخزين وإرسال المعلومات. في الشركات العائلية الصغيرة قد يكون نظام تقنية المعلومات بسيطاً مثل جدول بيانات إكسل. أما في الشركات الأكبر قليلاً فإن نظام تقنية المعلومات يأتي بشكل برمجيات مخصصة مثل برنامج (QuickBooks)، أما في الشركات الأضخم فإن نظام تقنية المعلومات يأتي بشكل تطبيقات شاملة للمؤسسة مثل نظام تخطيط موارد المؤسسات (ERP system). وفي الشكل (٤-١) يظهر نظام تقنية المعلومات على هيئة وعاء يحمل الأصول المعلوماتية.

الثغرات:

أصبح أمن المعلومات مهماً لأن جميع الأنظمة تحتوي على ثغرات. والثغرات هي نقاط ضعــف في أمن المعلومات تعطي التهديدات الفرصة بأن تصبح خطراً على الأصول[1]. ففي حالة نُظم تقنية المعلومات القائمة على برنامج مايكروسوفت إكسل والتي تم ذكرها أعلاه، تشــمل الثغرات الوصول غير المصرح به والذي قد يؤدي إلى فقدان الخصوصية أو التأثير في التكامل، كما تشــمل تعطل القرص الصلب الذي يؤدي إلى فقــدان الجاهزية. وإذا وصلنا إلى حالة من المثالية التي لا يوجد فيها أي ثغرة في نظم تقنية المعلومات، فلن يكون هناك حاجة لدراسة أمن المعلومات، ولن نحتاج إلى كادر من المهنيين المحترفين في أمن المعلومات. لكن منتجات البرمجيات الحديثة كبيرة. على ســبيل المثال يحتوي نظام ويندوز فيستا على مــا يقارب من ٥٠ مليون خط من التعليمات البرمجية[2]. ومن الصعب التنبؤ والقضاء على جميــع الثغــرات المحتملة في مثل هذه المنتجات الكبيرة. ويتم إنشــاء ثغرات إضافية عند التفاعــل بــين المنتجات، وحتى لو تم القضــاء على جميع ثغرات البرمجيــات فإن الثغرات التي ينشــئها المستخدم ستبقى. على ســبيل المثال لا يقوم الكثير من المستخدمين بحماية حساباتهم التنفيذية بكلمات مرور جيدة.

وللتعامــل مع الثغرات فــإن صناعة البرمجيــات بالتعاون مع الحكومــة الفدرالية قد اســتثمرت موارد كبيرة لإنشاء مخزون بالثغرات المعروفة للبرمجيات. وهذا المخزون يُعرف بقائمة التعرض والثغرات الشائعة (Common Vulnerabilities and Exposures) والتي تهدف إلى تحديد المُعرِّفات والأســماء الشــائعة لجميع ثغرات البرمجيات المعروفة للعامة. وهذه القائمة تحت إشراف مؤسسة ميتر (Mitre)، وهي مؤسسة بحوث وتطوير غير ربحية ممولــة مــن الحكومة الفدرالية. ويوضح الشــكل (٤-٢)[3] مثالاً للثغــرات في هذه القائمة (مُحدَّثة في تاريخ إعداد هذا التقرير).

---

(١) هذا تعريف مُبسط مأخوذ من الوثائق التقنية. على سبيل المثال، تُعرّف الثغرات في قاموس مصطلحات أمن الإنترنت (RFC 2828) بأنها «عيوب وثغرات في تصميم الأنظمة أو تطبيقها أو عملياتها أو إدارتها، والتي يمكن استغلالها لانتهاك سياسة أمن المعلومات»

(2) http://www.nytimes.com/2006/03/27/technology/27soft.html?pagewanted=all&_r=0

(3) http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2012-0779

بالنظر إلى النظام المحاسبي المستند إلى جداول البيانات في إحدى شركات الأعمال الصغيرة والذي تم ذكره أعلاه، في رأيك ما أهم ثغرات أمن المعلومات في هذا النظام؟

الشكل (٤-٢): مثال على قائمة التعرض والثغرات الشائعة (محدثة في تاريخ إعداد هذا التقرير)، مؤسسة ميتر (Mitre)

CVE-ID	
CVE-2012-0779 (under review)	Learn more at National Vulnerability Database (NVD) • Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings
Description	
** RESERVED ** This candidate has been reserved by an organization or individual that will use it when announcing a new security problem. When the candidate has been publicized, the details for this candidate will be provided.	
References	
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.	
Status	
Candidate	This CVE Identifier has "Candidate" status and must be reviewed and accepted by the CVE Editorial Board before it can be updated to official "Entry" status on the CVE List. It may be modified or even rejected in the future.
Phase	
Assigned (20120118)	
Votes	
Comments	

Candidate assigned on 20120118 and proposed on N/A

SEARCH CVE USING KEYWORDS: Submit
You can also search by reference using the CVE Reference Maps.

FOR MORE INFORMATION: cve@mitre.org

الشكل (٤-٣): بند (قاعدة البيانات الوطنية للثغرات)[٤] المقابل لـ (قائمة التعرض والثغرات الشائعة)

Vulnerability Summary for CVE-2012-0779

Original release date: 05/04/2012

Last revised: 05/04/2012

Source: US-CERT/NIST

This vulnerability is currently undergoing analysis and not all information is available.

Please check back soon to view the completed vulnerability summary.

Overview

Adobe Flash Player before 10.3.183.19 and 11.x before 11.2.202.235 on Windows, Mac OS X, and Linux; before 11.1.111.9 on Android 2.x and 3.x; and before 11.1.115.8 on Android 4.x allows remote attackers to execute arbitrary code via a crafted file, related to an "object confusion vulnerability," as exploited in the wild in May 2012.

References to Advisories, Solutions, and Tools

By selecting these links, you will be leaving NIST webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. NIST does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, NIST does not endorse any commercial products that may be mentioned on these sites. Please address comments about this page to nvd@nist.gov.

External Source: CONFIRM

Name: http://www.adobe.com/support/security/bulletins/apsb12-09.html

Hyperlink: http://www.adobe.com/support/security/bulletins/apsb12-09.html

(4) https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-0779

وبالإضافـة إلى أن المجتمع مهتم بأن يتم لفـت انتباهه إلى الثغرات الأمنية، فإن معظم المســتخدمين يرغبون كذلـك في التعرف على التأثيرات المحتملة للثغـرات والتدابير الموصى بهـا لإزالة تلك الثغرات. وبعـد جهد كبير، يتم الاحتفاظ بهذه المعلومات في قاعدة بيانات الثغرات الوطنية (National Vulnerabilities Database). ويمكنك مشاهدة الرابط من (قائمة التعرض والثغرات الشائعة) إلى (قاعدة البيانات الوطنية للثغرات) في الشكل (٤-٢). ويوضح الشــكل (٤-٣) إدخال (قاعدة البيانات الوطنية للثغرات) المقابل لـ (قائمة التعرض والثغرات) في الشكل (٤-٢).

وبعـض مواصفـات قائمة الثغرات أعلاه جديـرة بالملاحظة. ويتم إضافـة الثغرات إلى قاعدة البيانات بعد الإعلان عنها على الإنترنت. والمســؤول عن الإعلان هو الشركة الموردة للبرمجيـات. ويمكن العثور على مزيد من المعلومات حـول الثغرات على الموقع الإلكتروني لمـورد البرمجيات، وذلك باتباع الرابط الموجود في (قائمة التعرض والثغرات الشـائعة). ولا تقوم كل من (قائمة التعرض والثغرات الشائعة) و(قاعدة البيانات الوطنية للثغرات) بكشف الثغرات، بل يتمثل دورها الأسـاسي في العمل كمســتودع مركـزي لجميع الثغرات التي تم الإبلاغ عنها، وعادة ما يتم الكشف أولاً عن تلك الثغرات من قبل الشركة الموردة للبرمجيات.

	الثغرات الجديدة	الهجمات
٢٠١٠	٦٢٥٣	٣ مليارات
٢٠١١	٤٩٨٩	٥,٥ مليارات

المصدر: سيمانتيك (Symantec).

ونظـراً للعدد الكبير من منتجات البرمجيات المســتخدمة والحجـم المتزايد للبرمجيات الحديثة فإنه ليس من المســتغرب أن تكون (قاعدة البيانات الوطنية للثغرات) نشطة جداً. ففي شــهر مايو من عام ٢٠١٢ كان متوســط الثغرات التي تم الإبلاغ عنها ١١ ثغرة يومياً. وفي الرابع من شهر مايو، وبعيداً عن الثغرات التي يتم الإبلاغ عنها يومياً، كان هناك بلاغات عن ثغرات من شركة (VMWare) وشركة (IBM). وجميع الثغرات الثماني التي تم الإبلاغ عنها في ذلك اليوم قامت شركات البرمجيات بالإعلان عنها أولاً.

وعــلاوة على ذلك يتــم في كل عام نشر أخطر ٢٥ خطأ من أخطاء البرمجيات والموجودة في قاعــدة البيانات تلك[٥]. وعــلى اعتبار أن هذه النشرة مفصلة وشــاملة، فإنه يتم توفير عينات من التعليمات البرمجية والحلول المقترحة لكل من الثغرات التي تم تحديدها، وذلك لتســهيل المهمة على المطورين. وسنقوم باستخدام عينات من التعليمات البرمجية من تلك النشرة لاحقاً في هذا الفصل.

ويبدو أن الجهود قد أثمرت، فوفقاً لشركة ســيمانتيك (Symantec)، وهي الشركة التي تطور العديد من منتجات أمن المعلومات الشائعة، فقد تم اكتشاف ٤٩٨٩ ثغرة جديدة في عام ٢٠١١ مقارنة بـ ٦٢٥٣ في عام ٢٠١٠، وبنسبة انخفاض تقارب ٢٠٪[٦]،[٧].

التهديدات:

الثغــرات الموجودة في الأصول تُنشــئ التهديدات. وتُعرّف التهديــدات بأنها القدرات والنوايا وأساليب الهجوم من الأعداء لاستغلال أو الإضرار بالأصول. في مثال الإكسل السابق، قد يرغب الموظف في استغلال عدم وجود حماية للملف بكلمة مرور ويقوم بتغيير مُعدل راتبه في الساعة. وتَظهر التهديدات في النموذج الأساسي لأمن المعلومات (الشكل ٤-١) على شكل أسهم.

لقد تغيرت طبيعة التهديدات بشكل كبير في السنوات الأخيرة. في الأيام الأولى للإنترنت كانــت معظم التهديدات من باب المزاح والمقالب مثل تلك التي ارتكبتها عصابة ٤١٤. وفي بداية عام ٢٠٠٠ أصبحت التهديدات أكثر تخريباً وانتشــاراً (مثل فايروس ILOVEYOU). ولقد استجابت الصناعة ومجتمع المستخدمين لذلك بالحد من ثغرات البرمجيات، وتحسين تدريب المســتخدمين. وتشــير التوجهات في عــام ٢٠١١ إلى أن التهديدات المتبقية موجهة للغاية ودوافعها تجارية.

---

(5) https://www.sans.org/top25-software-errors/

(٦) تقرير سيمانتك عن تهديدات أمن الإنترنت. اتجاهات عام ٢٠١٠.

(٧) تقرير سيمانتك عن تهديدات أمن الإنترنت. اتجاهات عام ٢٠١١.

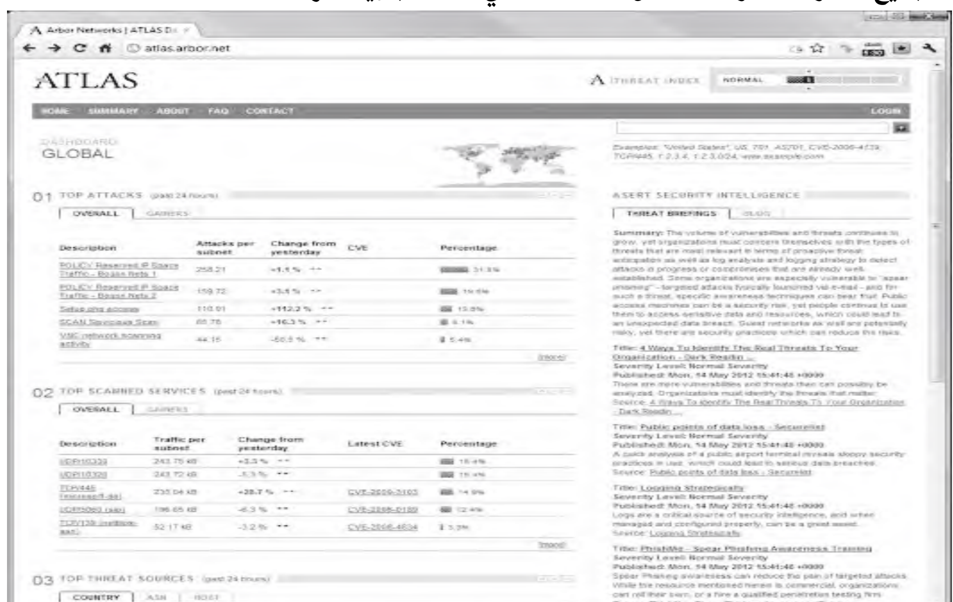
وقد قامت الصناعة بتطوير أداة تدعى أطلس (ATLAS)[٨] وهي أداة شائعة تُستخدم في تصور التهديدات الهامة التي تواجه المنظمة. ويستخدم أطلس (ATLAS) أجهزة الاستشعار المنتشرة من قبل مزودي خدمات الإنترنت في جميع أنحاء العالم لجمع المعلومات حول التهديدات التي تواجهها المنظمات في الوقت الفعلي لحدوث التهديد، ومن ثم تتم معالجة هذه المعلومات وعرضها على شبكة الإنترنت. ويمكن لمسؤولي الأنظمة التعرف بسرعة على الهجمات، والتأكد من أن لديهم الدفاعات المناسبة لمواجهة هذه الهجمات. ويوضح الشكل (٤-٤) واجهة أطلس على الإنترنت.

وفي شهر إبريل من عام ٢٠١٢ أصدرت سيمانتيك (Symantec) تقرير التهديدات لعام ٢٠١١ حيث منعت منتجات الشركة ٥,٥ مليارات هجمة في عام ٢٠١١، مقارنة بـ ٣ مليارات هجمة في عام ٢٠١٠، أي بزيادة قدرها أكثر من (٨٠٪). ومن المفارقات أنه في حين أن البرمجيات أصبحت أكثر أماناً، وعدد الثغرات أخذ في التناقص، إلا أن عدد الهجمات أخذ في الازدياد.

هذا التناقض ظهر بسبب ما يُعرف بـ «صناعة الهجوم» حيث ظهرت أدوات وبيئات تطويرية متكاملة مثل (Zeus, Spyeye) تساعد المهاجمين على إنشاء هجمات جديدة وسريعة، وتساعد على استغلال الثغرات الموجودة بكفاءة أكبر. إن إحداث هجمات ناجحة يحتاج فقط إلى خبرة قليلة باستخدام تلك الأدوات بدلاً من استخدام المبادئ الأولية، لذلك أصبحت التهديدات قابلة للاستغلال لأنها في متناول عدد أكبر من الناس. ولعل هذا يفسر إلى حد ما زيادة الهجمات المدفوعة بدوافع سياسية. وتلك هي بيئة أمن المعلومات التي نعيش فيها اليوم.

(8) https://atlas.arbor.net/about/

الشكل (٤-٤): واجهة أطلس على الإنترنت. تم الحصول على هذه المعلومات من (Arbor Networks' ATLAS Initiative) في تاريخ ١٢/مايو/٢٠١٢، ولقد تم الحصول على إذن لإعادة النشر. البيانات من موقع أطلس متغيرة ولذا فإنه قد تكون المعلومات الموجودة في الشكل تغيرت منذ تاريخ نشر البيانات. جميع الحقوق محفوظة. أطلس (ATLAS) هي علامة تجارية لشركة (Arbor Networks, Inc).



الضوابط:

ســتكون جميع أنظمة تقنية المعلومات معرضة للهجوم في المستقبل المنظور. وفي هذا الإطار الزمني ســيكون هناك مهاجمون متفرغون للتهديد باســتغلال تلك الثغرات الأمنية، وذلك لتحقيق مكاســب شــخصية أو بهدف دوافع أخرى. ما الذي يفعله مســؤول النظام للدفاع عن أجهزة الكمبيوتر التي في عهدته؟

يتمثــل دور أمن المعلومات في الحد من تلك التهديدات. ويتم ذلك عن طريق تطبيق الضوابــط الأمنيــة في أنظمة تقنيــة المعلومات المعرضــة للخطر. والضوابــط الأمنية هي الإجــراءات الوقائية المُســتخدمة للحد مــن تأثير التهديدات. وفي النموذج الأســاسي لأمن المعلومات (الشكل ٤-١) تظهر هذه الضوابط على شكل حلقة حول نظام تقنية المعلومات. وفي الشــكل (٤-١) يُشير عرض السهم الى التكرار النســبي لفئات التهديدات المُختلفة التي

تعرضت لها منظمة تقليدية. ويتم تعطيل مُعظم التهديدات باستخدام الضوابط المُعتمدة عادة لدى المنظمات. على سبيل المثال، تأتي معظم أنظمة التشغيل الآن مع جدار حماية تم ضبطه مع بعض الإعدادات الافتراضية التي تشجع المستخدم على استخدام كلمة مرور قوية لتأمين حساب المستخدم التنفيذي على أجهزة الحاسب الآلي الخاصة بهم. وتجارياً حتى الشركات الصغيرة تقوم بالنسخ الاحتياطي للملفات الهامة على محركات أقراص صلبة خارجية أو باستخدام خدمات الإنترنت الأخرى، كما تقوم بالحفاظ على أجهزة الحاسب الآلي الخاصة بها وحمايتها لمنع الوصول غير المصرح به.

فيما سبق قمت بتحديد الثغرات في النظام المحاسبي المستند إلى جداول البيانات. في رأيك ما أفضل وسيلة لحماية هذا النظام من تلك الثغرات؟

وحتى الضوابط البدائية المذكورة أعلاه يمكنها بنجاح منع غالبية التهديدات التي تواجه المنظمات. وهذه موضحة بالسهم العريض في الجزء السفلي من الشكل (٤-١).

لكن وكما هو موضح في الشكل (٤-١) حتى الضوابط الأمنية المُثلى تحتوي على فجوات. على سبيل المثال، يفضل المستخدمون عادة كلمات المرور التي لا تنسى على تلك الأكثر أمناً. كما أن المستخدمين عادة غير منتظمين في القيام بالنسخ الاحتياطي لملفاتهم حتى لو كان لديهم أنظمة نسخ احتياطي بآلاف الدولارات. وتقوم التهديدات باستغلال الثغرات الموجودة في الضوابط الأمنية للوصول إلى نظم تقنية المعلومات الضعيفة. وهذه التهديدات موضحة بأسهم على يمين الشكل (٤-١) والتي اخترقت الضوابط ووصلت إلى نظام تقنية المعلومات. ولحسن الحظ فإن تلك التهديدات قد لا تضر النظام حالياً، وهذه الفكرة موضحة بعدم قدرة السهم في الشكل (٤-١) للوصول إلى نظام تقنية المعلومات.

وبالعودة لنظام تقنية المعلومات القائم على جداول بيانات إكسل فإن أحد التهديدات هو سرقة جهاز الحاسب الآلي المحمول الذي تحتفظ الشركة فيه بسجلاتها. وفي كثير من الحالات يكون اللص راغباً في بيع جهاز الحاسب الآلي المحمول من أجل المال، ويقوم المشتري بإعادة تثبيت نظام التشغيل للمحافظة على أداء الجهاز. وفي هذه الحالة، ورغم أن المعلومات معرضة لخطر السرقة، فإن الخصوصية لم يتم اختراقها. وإذا كان لدى الشركة نظام جيد للنسخ الاحتياطي فإن الجاهزية أيضاً لن تتأثر.

لكن جزءاً صغير جداً من التهديدات سيسـبب ضرراً حقيقياً للمنظمة. وسـتنجح هذه التهديدات في التغلب على الضوابط الأمنية السـابقة واستغلال الثغرات لاختراق المعلومات المرغوب فيها. هذه التهديدات موضحة بالسهم في الجزء العلوي من الشكل (٤-١). ومثال على ذلك من النظام المعتمد على جداول بيانات إكسـل هو وصول أحد الموظفين إلى جهاز الحاسـب الآلي المحمول عنـد عدم تواجد المدير وقيامه بتغيير عدد السـاعات التي عملها لزيادة تعويضه المالي.

وتدور مهنة أمن المعلومات حول منهجية تحديد أصول المعلومات، والثغرات، والتهديدات، والضوابط، ونشر الضوابط بشـكل مناسـب بحيث أن الأموال التي تُنفق على تلك الضوابط تحقق أكبر عائد ممكن للمنظمة. وما تبقى من هذا الكتاب يشرح تلك المكونات بالتفصيل حيـث يسـتعرض ما تبقى من هذا الفصل: الثغرات، والتهديـدات، والضوابط الهامة. وقد يُنظر إلى هذه الجزئية على أنها تمرين لبناء مفرداتك في أمن المعلومات.

> تستخدم أدبيات أمن المعلومات الشائعة عبارة «الثغرات»، و«التهديدات»، و«المخاطر» بشكل متبادل، وهذا أمر مؤسف. وتشمل المخاطر كلاً من إمكانية حدوث الخسائر وقياس الخسائر عند حدوثها. وترتبط الثغرات بالنصف الأول من المخاطر؛ لأنها تؤسس لإمكانية حدوث الخسائر. وترتبط التهديدات بالنصف الآخر من المخاطر - إذا كانت ناجحة فإن التهديدات ستؤدي إلى حدوث خسائر. ويهتم المديرون بتخفيف المخاطر. وتتحول التهديدات والثغرات إلى مخاطر فقط عندما تكون أصول المعلومات الثمينة في خطر.
>
> وخير مثال على ذلك وثيقة «تصنيف المخاطر التشغيلية لأمن الإنترنت» (A taxonomy of operational cyber security risks) من معهد هندسة البرمجيات (SEI) في جامعة كارنيجي ميلون (CMU). ومن المخاطر المحددة في الوثيقة «تصرفات الناس» والتي يتم تصنيفها عادة كثغرات[٩].
>
> وفي مثال النظام محاسبي المستند إلى جدول البيانات، قد يكون الخطر في عدم قدرة الشركة على سداد الديون بسبب قيام موظف مُستاء بالتلاعب في البيانات على جهاز الحاسب الآلي غير المحمي. والثغرة الأمنية في هذا المثال هي جهاز الحاسب الآلي غير المحمي، أما التهديد فهو الموظف المُستاء. وسنقوم بتغطية موضوع إدارة المخاطر بالتفصيل في الفصل الرابع عشر، حيث سنقوم في ذلك الفصل بكتابة بعض عبارات المخاطر وذلك للتمييز بوضوح بين المفاهيم الثلاثة، وذلك حتى يكون قُرّاء هذا الكتاب قادرين على التمييز بين «الثغرات»، و«التهديدات»، و«المخاطر»، واستخدام المصطلحات الصحيحة حسب الحاجة.

(9) http://resources.sei.cmu.edu/library/asset-view.cfm?assetid=9395

الثغرات، والتهديدات، والضوابط الشائعة:

خلال الفصول القادمة من هذا الكتاب سـوف نسـتعرض ضوابط أمن المعلومات الهامة بمزيد من التفصيل. وفي هذا الوقت فإنه من المفيد أن نعرض الثغرات والتهديدات والضوابط الأكثر شيوعاً حتى يمكنك البدء في التفكير في الأبعاد المختلفة لتحديات أمن المعلومات.

الثغرات الأمنية:

الثغـرات هي النقاط التي يمكن اسـتغلالها في نظم المعلومات. وتوجد ثغرات لا حصر لها كما يتم اكتشـاف ثغـرات جديدة كل يوم. ولفهم الثغرات بطريقة مناسـبة لا بد من تصنيفهـا بطريقـة ما، وفي الواقع هناك العديد من أنظمة التصنيف للثغرات. على سـبيل المثال، يقوم أحد أنظمة التصنيف بتقسـيم الثغرات بناءً على مرحلة دخول الثغرة في دورة حياة تطوير البرمجيات (software development life cycle). وتقوم مجموعة من طرق التصنيف الأخرى بتصنيف الثغرات بناءً على التهديدات التي تُنشـئها. وللأسف فإن جميع طرق التصنيف تلك تعاني من بعض السلبيات. على سبيل المثال، في نظم المعلومات الكبيرة يعاني نظام التصنيف القائم على دورة حياة تطوير البرمجيات من صعوبة التحديد الدقيق للمرحلـة التي تم فيها دخول الثغرة. أما أنظمـة التصنيف القائمة على تحديد التهديدات التي تنشـئها الثغرات فإن آلية التصنيف حتماً غير مكتملة بسـبب أن هناك أنواعاً جديدة من التهديدات تُكتشف في كل وقت(١٠).

ولتحقيـق أهداف هذا المقرر الدراسي فإنه من المناسـب تصنيـف الثغرات إلى ثغرات برمجية، وثغرات إجرائية.

الثغرات البرمجية:

الثغـرات البرمجية هي أخطاء في مواصفات أو تطوير أو ضبط البرمجيات بحيث ينتهك تنفيذ تلك البرمجيات سياسة الأمان(١١). وفيما يلي نعرض بعضاً من الثغرات البرمجية الأكثر شيوعاً:

---

(10) Meunier, P. Classes of vulnerabilities and attacks (download). In: Handbook of Science and Technology for Homeland Security, Wiley, 2007

(11) Krsul, I. "Software vulnerability analysis." unpublished PhD dissertation, Purdue University, 1988.

عدم التحقق من صحة المدخلات: الثغرات المتعلقة بالتحقق من صحة المدخلات ترجع إلى الحالة التي يتم فيها استخدام مدخلات المُستخدِم في البرنامج دون التأكد من صحتها. والاستخدام الشـائع للبرمجيات، وبالأخص برمجيات الإنترنت، هـو الوصول للمعلومات من قواعد البيانات. من الأمثلة على ذلك استرجاع قوائم الأفلام في مواقع الإنترنت مثل موقع (sonypictures.com)، أو استرجاع نص صفحة إنترنت من أنظمة إدارة المحتوى (content management systems) في مواقع الإنترنت مثل موقع (PBS Frontline) وموقع (HB Gary)، وهي شركة أمن للحاسـب الآلي تقوم بتوفير حلول أمنية متخصصة لعدة أجهزة حكومية. وعادة ما يقوم مسـتخدمو هذه المواقع باسـتخدام مربع البحث أو غيرها من حقول الإدخال لتحديد احتياجاتهم من المعلومـات، وبعد ذلك تقوم البرمجيات التـي تعمل في الموقع الإلكتروني بمعالجة مدخلات المستخدم لتوفير الاستجابة المناسبة. وإذا لم يتم التحقق من صحة إدخال المستخدم بشكل صحيح فإن المسـتخدم يسـتطيع الوصـول إلى معلومات يُفترض ألا يحصـل عليها. وفيما يلي مثال لتعليمات برمجية لأحد البرامج باسـتخدام استعلام باللغة الاستفسارية الإنشائية المركبة (SQL) لإيجاد العناصر المطابقة لاسم المستخدم واسم العنصر. وإذا لم يتم التحقق من صحة مدخلات المُستخدم فإن المستخدم يستطيع الحصول على جميع العناصر المذكورة في جدول العناصر[١٢].

```
query = "SELECT * FROM items WHERE itemname = ' " + ItemName.Text + " ' ";

// expected user input for ItemName:  pencil;

// actual user input for ItemName:  pencil OR 'a'='a';

// query result is:

SELECT * FROM items WHERE itemname = pencils OR 'a'='a';

// which translates to:

SELECT * FROM items;
```

والعامل المشترك بين المواقع الإلكترونية المذكورة هنا (PBS Frontline) و (HB Gary Federal) و (Sony Pictures) هـو أنها تعرضـت للاختراق بطريقة محرجة في عام ٢٠١١ وذلك بسبب عدم قيام برمجيات الإنترنت من التحقق من صحة المدخلات.

(12)http://cwe.mitre.org/top25/index.html#CWE-89

النمــوذج المحدد للثغــرات المتعلقة بالتحقق من صحة الإدخــال في المثال أعلاه يُدعى «ثغرات حقن اللغة الاستفسـارية الإنشـائية المركبــة» (SQL injection vulnerability) ويقصد بها استخدام مدخلات لغة الـ (SQL) غير المُتَحَقق منها في التطبيقات.

رفــع الملفات غير المقيد: يحدث رفع الملفات غير المقيــد عندما يتم قبول الملفات من قبل البرمجيات دون التأكد من أن الملف يتبع مواصفات دقيقة. على ســبيل المثال، تشجع العديد من مواقع التجارة الإلكترونية المســتخدمين على رفع صور لاســتخدامهم للمنتجات التــي تم شراؤها عن طريق الموقع. وإذا كانت تلك المواقع لا تقوم بالتحقق من أن الصور التــي تم رفعها هي بالفعل مــن امتداد (jpg) أو امتــداد (gif) أو غيرها من صيغ ملفات الصــور المماثلة، فإنه من الممكن للمهاجمين أن يقوموا برفع برمجيات على الموقع بدلاً من رفــع الصــور. ومن ثَمّ تقوم تلك البرمجيات بمحاولة اخــتراق الموقع، مثلاً عن طريق سرقة أسماء المستخدمين وكلمات المرور.

ولمنع مثل هذه الهجمات من الحدوث، من المستحســن أن تُعامل جميع الملفات التي يتم رفعها من قبل المستخدمين على أنها ملفات خبيثة، ومن ثم يتم البحث فيها عن رموز الملفــات الضــارة. وهذا البحث لا يعد عديم الفائــدة إذ إن جميع الملفات (كملفات gif) تحتوي على حقول للملاحظات والتي قد يستخدمها المهاجمون لإخفاء الرموز الضارة.

البرمجة النصية المشــتركة للمواقع الإلكترونية: وتحدث البرمجة النصية المشــتركة عند اســتخدام المدخلات المُعدة من قبل المستخدم دون التحقق من سلامتها بوصفها جزءاً من المخرجات المُقدمة لمستخدمين آخرين. وتُوصف هذه الطريقة بأنها «ثغرة» لأنها الطريقة الأكثر شــيوعاً التي يتم اســتغلالها من قبل المهاجمين للوصول إلى الضحايا الذين يتصفحون موقعاً ما، حيث يقوم المهاجم بتزويد إحدى شــفرات جافا سكريبت الخبيثة (scripting) كمدخلات إلى مســتخدم آخــر على الموقع المُســتهدف وهو «الموقع الإلكتروني المشــترك» (cross-site). ولتوضيح هذه الثغرة، نســتعرض المثال التالي وهو من قاعدة بيانات أخطر ٢٥ خطأً من أخطاء البرمجيات التي تم ذكرها آنفاً.

تأمل في صفحة بسيطة لموقع إلكتروني مكتوبة بلغة الـ (php) على النحو التالي:

```
$username = $_GET['username'];

echo '<div class="header"> Welcome, ' .  $username .  '<\div>';
```

وتهدف هذه الصفحة لأخذ اســم المســتخدم من نموذج الصفحة السابقة أو عنوان الموقع المنتهي بـ (?username = John) لإنشاء رسالة ترحيبية للمستخدم مثل (Welcome, John).

http://trustedSite.example.com/welcome.php?username=<script

Language="Javascript"> alert ("You've been attacked! ") ;<\Script>

والســطر الأخير سيعرض مربع حوار تنبيهي للمستخدم. وحتى يتم عرض مربع الحوار نفســه لمستخدم آخر، يقوم المهاجم بإرســال بريد إلكتروني للضحية بعنوان الموقع المناسب. وعندما يقوم الضحية بالنقر على البريد الإلكتروني، سيتم عرض مربع الحوار التنبيهي للضحية.

وفي المثال أعلاه لا يحدث أي ضرر، لكن المهاجم الحقيقي يستطيع استغلال هذه الثغرة لحث الضحية على تفعيل مزيد من الأكواد الأكثر ضرراً. والبرمجة النصية للمواقع المشتركة هي من أكثر الثغرات شيوعاً لتطبيقات الإنترنت لدرجة أن لها اختصاراً خاصاً بها وهو (XSS). وهذه الثغرة موجودة بشــكل أو بآخر في المواقع الإلكترونية الواســعة الانتشار بما في ذلك الأسماء المشــهورة كـ (Facebook)، و (Barracuda Spam Firewall)، و (Mediawiki) وهو الموقع الأساس لموقع ويكيبيديا، وغيرها من المواقع الإلكترونية المشهورة.

تجاوز ســعة المخزن المؤقت: ويقصد بـ (تجاوز سعة المخزن المؤقت) الحالة التي يقوم فيها برنامج ما بوضع كمية من كبيرة من البيانات أكبر من ســعة المخزن، وهذه واحدة من ثغرات البرمجيات الشــائعة. وعادة ســتؤدي مثل هذه الحالة إلى تحطم البرمجيات. لكن المهاجــم، الذي لديه معرفة تفصيلية عن البرنامج، يســتطيع حقن بعض المدخلات الخاصة بحيث تقوم المحتويات الفائضة باختراق جهاز الحاسب الآلي بطرق يُمكن توقعها. ويسمح الاختراق عادة للمهاجمين بالاتصال بجهاز الحاسب الآلي عن بعد ومن ثم سرقة المعلومات.

ويُعــد (تجاوز ســعة المخزن المؤقت) منتشراً في البرمجيــات المكتوبة بلغات برمجة غير مُــدارة (unmanaged languages) كلغــة (C) و (++ C). وتقــوم لغات البرمجة المُدارة (managed languages) مثل (Java) و(# C) بإدارة الذاكرة والبيانات بحيث يكون (تجاوز ســعة المخزن المؤقت) غير ممكن في البرمجيات المكتوبة بهذه اللغات. لكن يتم كتابة أكثر البرمجيــات (بما في ذلك المتصفحات الحديثة مثل كــروم وفايرفكس) بلغة (++ C/C) من أجل تحقيق التوافق عبر المنصات المتعددة[١٣]. لذلك فإن القضاء على (تجاوز سعة المخزن المؤقت) في معظم التطبيقات الحديثة يتطلب مهارات برمجة دقيقة للغاية.

(١٣) لمزيد من المعلومات بالإمكان استعراض التعليمات البرمجية لمتصفح كروم على الرابط: https://src.chromium.org/viewvc/chrome/trunk/src/chrome/browser/?sortby=file

الأذونات الناقصة: وتحدث ثغرة الأذونات الناقصة عندما يسمح البرنامج للمستخدمين بالوصول إلى أجزاء متميزة من البرنامج دون التحقق من بيانات اعتماد المستخدم. ودائماً يحاول المهاجمون العثور على أجزاء من النظام المالي التي يمكن الوصول إليها دون الحاجة لبيانات الاعتماد. وإذا تم العثور على هذا الجزء، فمن المرجح أن يتم استغلاله لسرقة معلومات مالية حساسة. وفي الواقع فإن العديد من حالات سرقة البيانات الكبيرة التي حدثت هي نتيجة لثغرة الأذونات الناقصة. على سبيل المثال، ووفقاً لنشرة «أخطر ٢٥ خطأ» فإن مئات الآلاف من الحسابات البنكية التابعة لـ (Citigroup) قد تعرضت للاختراق في شهر مايو من عام ٢٠١١ نتيجة لوجود ثغرة الأذونات الناقصة.

البيانات غير المشفرة: وتحدث ثغرة (البيانات غير المشفرة) عندما يتم تخزين بيانات حساسة محلياً أو عندما يتم نقلها عبر الشبكة بدون التشفير السليم. وتشمل البيانات الحساسة بيانات اعتماد المستخدم وغيرها من المعلومات الخاصة. ويمكن قراءة البيانات غير المشفرة والمتدفقة عبر الشبكة بسهولة باستخدام برامج تُدعى (sniffers). ويمكن سرقة البيانات غير المشفرة والمخزنة في قاعدة البيانات إذا سمحت (الأذونات الناقصة) أو (عدم التحقق من صحة المدخلات) للمستخدمين بقراءة البيانات. وتمثل (البيانات غير المشفرة) عنصراً من عناصر سرقة البيانات الرئيسية.

الثغرات الإجرائية:

الثغرة الإجرائية هي عبارة عن ضعف في الطُرق التشغيلية للمنظمة والتي يمكن استغلالها لانتهاك السياسة الأمنية. ويُمكن عن طريق الثغرات الإجرائية اختراق المعلومات حتى لو تمت إزالة جميع الثغرات البرمجية. وأهم أنواع الثغرات الإجرائية ما يلي:

إجراءات كلمة المرور: حماية كلمة المرور هو الإجراء الموحد المستخدم لتقليل تأثير العديد من الثغرات البرمجية بما في ذلك (الأذونات الناقصة)، و(عدم التحقق من صحة المدخلات)، و(رفع الملفات الغير مقيد). والمطلوب من المستخدمين إنشاء كلمات مرور معروفة لهم فقط، ولا يُسمح للمستخدمين بالوصول إلى المعلومات الحساسة إلا بعد إدخال كلمات المرور تلك. لكن كلمات المرور قد لا توفر الأمن الكافي إذا لم تكن المنظمة دقيقة حول الإجراءات المرتبطة بكلمات المرور.

على ســبيل المثال، إذا كانت كلمة المرور قصيرة جداً (مثل، «abcd»)، أو سهلة التخمين (مثــل، «password»، أو «admin»)، أو تعتمــد على كلمة موجــودة في القاموس (مثل، "computer")، أو تستخدم جزءاً من بيانات المستخدم (مثل، «John») فإنها لا توفر الكثير مــن الحماية. وفي حالة التحدي لمعرفــة كلمة المرور فإن المهاجمين عادة يجربون تركيبات مختلفة من كلمات المرور تلك.

ولأن هذا الموضوع يُعد مصدر قلق ســائداً فإن الكثير من مزودي البرمجيات يسمحون لمسؤولي النظم بتحديد إجراءات كلمات المرور لمنع استخدام كلمات المرور الضعيفة.

نصائح لكلمات المرور الجيدة

من المستحسن استخدام كلمات مرور جيدة في الحياة الشخصية. ومن نصائح الحصول على كلمات مرور جيدة ما يلي[١٤]:

١. الطول: استخدم كلمة مرور تتكون من ثمانية رموز على الأقل.

٢. التعقيد: استخدم كلمة المرور تتكون من أرقام وحروف ورموز وعلامات الترقيم. كلمات المرور الطويلة والمعقدة من الصعب اختراقها.

٣. التغيير: قُم بتغيير كلمة المرور بشكل منتظم بحيث أنه حتى لو تم اختراق كلمة المرور فإن هذه الثغرة ستزول تلقائياً.

٤. التنويع: استخدم كلمة مرور مختلفة لكل موقع إلكتروني. وعلى أقل تقدير قم باستخدام اثنتين من كلمات المرور- واحدة للمواقع الإلكترونية الحساسة (مثل مواقع البنوك ومواقع المحلات التجارية) والأخرى لمنتديات الإنترنت، وغرف الدردشة، وغيرها من المواقع الأقل حساسية. ويقوم المهاجمون عادة بسرقة بيانات الاعتماد من المواقع الإلكترونية الأقل حساسية (والتي غالباً لا يتم تصميمها بعناية) ومحاولة استخدام بيانات الاعتماد في المواقع الإلكترونية الحساسة مثل مواقع البنوك ومواقع المحلات التجارية. وللحصول على معلومات مثيرة ومفصلة حول مثل هذه الحوادث اقرأ تجربة جيمس فالوز (James Fallows) المراسل الوطني لمجلة (The Atlantic) والكاتب السابق لخطابات الرئيس الأمريكي جيمي كارتر[١٥].

(14) www.microsoft.com/security/online-privacy/passwords-create.aspx

(15)http://www.theatlantic.com/magazine/archive/2011/11/hacked/308673/

إجراءات التدريب:

كلما زاد مستوى أمن البرمجيات ركز المهاجمون على عفوية المستخدم النهائي. فالمهاجم قد يرسل رسائل إلكترونية قد تبدو أنها من الرئيس التنفيذي للمنظمة لكنها في الواقع تستخدم طريقة البرمجة النصية للمواقع المشتركة (XSS-cross-site scripting) أو طرقاً أخرى للحصول على بيانات اعتماد المستخدم. بعد ذلك يتمكن المهاجم من استخدام بيانات الاعتماد تلك لتجاوز حماية كلمات المرور والوصل إلى المعلومات الحساسة. وعلى أقل تقدير فإن على المنظمة أن تُعلن بشكل واضح أنها لن تقوم مطلقاً بإرسال رسائل إلكترونية مُتطفلة تطلب من المستخدمين كلمات المرور أو بيانات الاعتماد، وأن مثل هذه الطلبات تتم بشكل رسمي، مثلاً عن طريق رسالة في البريد العادي، أو عن طريق إرسال مذكرة من خلال التسلسل الهرمي للمنظمة، وغيرها من الطرق الرسمية الأخرى.

الحد الأدنى لإجراءات تدريب أمن المعلومات

يجب على المنظمات اعتماد سياسة عدم سؤال الموظفين عن المعلومات الحساسة كاسم المستخدم وكلمة المرور من خلال البريد الإلكتروني أو المكالمات الهاتفية. ويجب على جميع الموظفين في جميع المستويات معرفة هذه السياسة. وعلى الموظفين أن يعلموا أن بإمكانهم التخلص من تلك الرسائل الإلكترونية بغض النظر عن مصدرها وبغض النظر عن ماهية الظروف.

التهديدات:

يمكن أن نملأ كتاباً كاملاً من خلال مناقشة جميع تهديدات أمن المعلومات. لكن بعضاً من تلك التهديدات اشتُهرت بسبب الخسائر التي أحدثتها على مدى سنوات، ومن ثم حصلت تلك التهديدات على شهرة خاصة في مجال أمن المعلومات. ولأنك ستصبح خبيراً في مجال أمن المعلومات فإنه من المستحسن أن تكون على علم بتلك التهديدات، والتي سيتم وصفها بإيجاز فيما يلي.

الفيروسات/ الدودة الحاسوبية: أكثر الناس على دراية بالفايروسات والدودة الحاسوبية، ومعظم أجهزة الحاسب الآلي التي تباع اليوم تأتي مع إصدارات تجريبية لبرامج مكافحة

الفيروســات. الفيروســات والدودة الحاســوبية هي برمجيات تؤثر سلباً في أجهزة الحاسب الآلي وتنتشر من خلال الشــبكة دون موافقة المستخدم. الفرق بين الاثنين هو أن الفايروس يســتخدم برمجيات أخرى للانتشــار (مثلاً برنامج البريد الشــخصي للمستخدم)، في حين أن الدودة تنتشر من تلقاء نفســها. ولأن مُنتجي الفايروسات والدودة الحاسوبية يعلمون بأن مســتخدمي الحاسب الآلي يستخدمون برامج لمكافحة الفيروســات فإن الدودة الحاسوبية والفيروسات الحديثة يتم تصميمها لإحداث أكبر ضرر ممكن في غضون دقائق من إطلاقها. على ســبيل المثال، تــم إطــلاق دودة ســلامر (Slammer worm) في الخامس والعشرين مــن يناير من عام ٢٠٠٣ من خلال اســتغلال ثغرة (تجاوز ســعة المخزن المؤقت) في خادم مايكروســوفت إس كيو إل (Microsoft›s SQL Server). وتم اكتشــاف الثغرة في شــهر يوليو من عام ٢٠٠٢، وبعد ذلك بوقت قصير أصدرت مايكروســوفت تحديثاً لتصحيح تلك الثغــرة. و عــلى الرغم من أن الأجهزة التي لم يتم فيها تصحيــح الثغرة هي المعرضة فقط للخطر فقد وصلت الدودة لـ (٩٠٪) من تلك الأجهزة المســتهدفة في أقل من ١٠ دقائق[١٦]، مما تســبب في إصابة أكثر من ٧٥,٠٠٠ جهاز. وفي قســم (نمــوذج الحالة) من هذا الفصل سيتم التعرض للقصة الممتعة لفيروس (ILOVEYOU).

رفــض الخدمــة (Denial of service): رفــض الخدمة هو المنع غــير المصرح به من الوصــول إلى الموارد أو تأخير العمليات الحساســة ذات الوقــت الحرج. ويتم تحقيق ذلك عــادة من خلال عمل عدد كبير من الطلبات غير الضرورية في نظام المعلومات. وبعد ذلك يتم إشــغال موارد النظام المســتهدف بتنفيذ الطلبات غير الضرورية، وذلك يمنع النظام من القدرة على الاســتجابة للطلبات المنطقية في الوقت المناسب. ويمكن تعزيز هجمات رفض الخدمــة عن طريق نشر أجهزة حاســب آلي متعددة لعمل تلــك الطلبات غير المصرح بها. وتسمى مثل تلك الهجمات بهجمات رفض الخدمة الموزعة وهي عبارة عن استخدام العديد من الأنظمة المخترقة لإحداث رفض الخدمة لمســتخدمي النظام المستهدف. ولحسن الحظ فإنه من الســهل نسبياً التعرف على ســيل الطلبات الواردة إلى هدف واحد وتشخيصه بأنه هجوم رفض الخدمة، ويمكن منع تلك الطلبات بسهولة من خلال مزودي خدمات الإنترنت.

(16) 6Moore, D.. Paxson, v..Savage, S., Shannon. c., Staniford, S., and Weaver, N. «Inside the Slammer worm,» IEEE Security and Privacy. July/ August 2003

ولمعلومات مفصلة ومفيدة وممتعة عن هجمات رفض الخدمة اقرأ تقرير ستيف جيبسون (Steve Gibson) عن هجمات رفض الخدمة ضد شركته(١٧).

الانتحال (Phishing): محاولة اختراق مستخدم ما عن طريق التنكر بصفة جهة موثوق بها في التواصل الإلكتروني يُسمى الانتحال. وتهدف هجمات الانتحال المبكرة للحصول على معلومات مثل اسم المستخدم، وكلمة المرور، وتفاصيل بطاقة الدفع الائتمانية. ويستلم أكثر الناس ما لا يقل عن واحدة إلى اثنتين من رسائل الانتحال الإلكترونية كل أسبوع. ويوضح الشكل (٤-٥) مثالاً على ذلك. وتظهر رسائل البريد الإلكتروني على أنها صادرة من البنوك، وتقود تلك الرسائل الإلكترونية المستخدمين لزيارة مواقع إلكترونية تبدو مثل مواقع البنوك الإلكترونية. وفي الموقع الإلكتروني يُطلب من المستخدمين إدخال اسم المستخدم وكلمة المرور بهدف إجراء بعض التصحيح في البنك. وفي حين تظهر رسائل البريد الإلكتروني والمواقع الإلكترونية على أنها حقيقية إلا أنها في الواقع ليست كذلك. فنظرة فاحصة إلى عنوان الموقع تبين أن الموقع تم استضافته على خادم مخترق. وفي الشكل (٤-٥) على سبيل المثال تم استضافة الموقع على موقع مدرسة في ولاية ألاباما.

وفي الآونة الأخيرة تم استخدام الانتحال في هجمات مركبة مع هجمات الهندسة الاجتماعية (social engineering) والاستغلال الفوري (zero-day exploits) لبدء تهديدات متطورة ومستمرة. وسيتم مناقشة الهجمات المرتبطة بشركة (RSA) والتي تمت في عام ٢٠١١ مع هجمات الاستغلال الفوري (zero-day exploits) في مثال في هذا القسم.

البرمجيات الخبيثة (Malware): البرمجيات الخبيثة مصطلح عام يُستخدم لوصف البرمجيات أو الرموز المصممة خصيصاً لاستغلال جهاز الحاسب الآلي أو البيانات التي يحتويها دون موافقة المستخدم. والطريقة الشائعة للبرمجيات الخبيثة للوصول إلى أجهزة الحاسب الآلي هي طريقة التحميل المجاني، وذلك عندما يقوم مصمم البرمجيات الخبيثة بإنشاء برمجيات تبدو أنها مفيدة جداً ويقوم بتوزيعها مجاناً.

(17) Gibson, S. "The strange tale of the denial of service attacks against GRC.com." http://www.crime-research.orgllibrary/grcdos.pdf (accessed 01/13/2012).

الشكل (٤-٥): مثال على الانتحال



وعندما يقوم المســتخدم الغافــل بتحميل وتثبيت تلك البرمجيــات المجانية التي تبدو أنها مفيدة فإنه يتم تثبيت تلك البرامج الضارة معها. وتُســمى هذه التقنية بتقنية حصان طروادة. وهناك أنواع عديدة من تلك البرمجيات الخبيثة بما في ذلك مسجل المفاتيح (key loggers)، وعمــلاء الزومبي (zombie clients)، وتقنية التحكم الخفي في جهاز الحاســب الآلي (rootkits). ومســجل المفاتيــح (key loggers) هو البرنامــج الذي يتعقب ضربات مفاتيــح لوحة المفاتيح في محاولة لجمع أســماء المســتخدمين وكلمات المــرور. أما عملاء الزومبي (zombie clients) فهو برنامج يتلقى الأوامر من جهاز حاسب آلي عن بعد بحيث يســيطر هذا البرنامج على جهاز الحاســب المصاب ويقوم من خلاله بأداء مهام ضارة وفقاً للتوجيهات التي يتلقاها. ويُطلق على جهاز الحاسب الآلي المصاب اسم زومبي. وتُستخدم الزومبــي عادة في إرســال الرســائل الإلكترونية غير المرغوب فيهــا، وإطلاق هجمات رفض الخدمة، واختراق أجهزة الحاســب الآلي في المنشآت الحساســة كالبنوك والقوات المسلحة.

وحصل الزومبي (أو الإنســان الآلي - الروبوت) على هذا الاســم لأنه يطيع الشــخص الذي يتحكم فيه طاعة عمياء.

تقنيــة التحكم الخفي في جهاز الحاســب الآلي (rootkits): وهي عبارة عن مجموعة مــن البرمجيات تُســتخدم لإخفــاء وجود البرامج الضارة في نظام الحاســب الآلي. ويشــير مصطلــح (rootkits) إلى أدوات البرنامــج التي تعطي المســتخدم وصولاً غير مصرح به إلى الجذر (والجذر-root-هو الحساب التنفيذي في أنظمة ينكس). كما تقوم هذه البرمجيات باســتبدال أدوات النظام القائمة (مثل تلك الأدوات التي تســتخدم لعرض العمليات-top- ومحتويات المجلدات -ls-)، ومن ثم فإن النســخة المعدلة مــن النظام تقوم بإخفاء وجود المســتخدم غير المصرح بــه. ويُعد تثبيت الــ (rootkits) في جهاز الضحيــة أحد أهداف البرمجيات الخبيثة.

وتُســتخدم الـ (rootkits) عادة من قبل المتســللين لإخفاء وجــود البرمجيات الخبيثة الأخرى مثل (عملاء الزومبي) حتى لا يعلم مالك جهاز الحاسب الآلي بأنه تم اختراق جهازه وأنه يُستخدم لإرسال رسائل إلكترونية غير مرغوب فيها أو أنه يُطلق هجمات رفض الخدمة.

ومــن بين جميــع تهديدات البرمجيات فإن الــ (rootkits) يُعد تهديــداً خطيراً، وذلك لقدرته على تدمير معايير حماية نظم التشغيل. ولهذا السبب فإنه من شبه المستحيل إزالة الـ (rootkits) من الجهاز المُخترق وأنه من المستحســن في هذه الحالة إعادة تثبيت نظام التشغيل بالكامل.

الاســتغلال الفــوري (zero-day exploits): ويتــم من خلالها اخــتراق ثغرة لم تكن معروفة في برمجيات الحاســب الآلي. ويُشــير المصطلح إلى أن المطورين لديهم (صفر) من الأيام لمعالجة الثغرة التي تم اســتغلالها. وعلى الرغم من أن المطورين ليس لديهم معرفة بالثغرة التي تم اســتغلالها وقت وقوع الهجوم، فإن شــخصاً ما كان على علم بتلك الثغرة وأُتيحت له الفرصة لتحديد وسيلة ما لاستغلال الثغرة بنجاح[١٨].

(18) يُوجد سوق لمثل ذلك الاستغلال كما في المصدر التالي. Greenberg, A. «Shopping for zero-days: a price list for hackers› secret software exploits,»http://www.forbes.com/sites/andy greenberg/20 shopping -for-zero-days-an-price-list -for-hackers-secretsoftware-exploits/ (accessed/23/03/12 (2212013/07

شكل (٤-٦): هجمة الاستغلال الفوري لبرنامج (Adobe Flash) والتي تم إطلاقها في ٢٠١١/٢/٢٨



وأحد هجمات الاستغلال الفوري (zero-day exploits) المشهورة ترتبط بشركة (RSA)، وهــي إحــدى الشركات الرائدة في تقنيــة رموز الأمــان (SecureID tokens)، وهي تقنية تســتخدم للتصديق الثنائي في بيئة المنظمات. ففي الســابع عشر من شــهر مارس من عام ٢٠١١ أعلنت الشركة أنه تم اختراق نظام تقنية المعلومات المســؤول عن توليد رموز الأمان مما يعني احتمالية اختراق أمن عملاء الشركة. ويعتقد الخبراء أن الاختراق كان نتيجة لهجمة الاستغلال الفوري المرتبط بتقنية برنامج (Adobe Flash)[١٩]. ومن المثير للاهتمام أنه بعد هذه الحادثة بـ ١٨ يوماً قام أحد المهاجمين على تويتر باستخدام المعرف (@yuangel975) بالإعلان عن إطلاق هجمة الاســتغلال الفوري المرتبطة ببرنامج (Adobe Flash) (الشــكل ٤-٦)، مما يثير الشكوك أنها الهجمة نفسها التي تم استخدامها في الحادثة[٢٠].

الزومبــي: وهو جهاز حاســب آلي متصل بالإنترنــت تم اختراقه لتنفيــذ المهام الضارة بتوجيــه من مُتحكِم عن بعد. وأتى اســم (زومبي) من الامتثال غــير المشروط للتوجيهات عــن بعد. وتُســمى الزومبي أحياناً بالإنســان الآلي (bots). وعموماً يكــون مالكو أجهزة الزومبي غافلين عن الاختراق حتى يتم إعلامهم من قبل مسؤولي الأنظمة. وهذا النوع من التهديــدات متوفر بتكلفة معقولة حيث يصل معــدل الإيجار لـ ١٠٠,٠٠٠ إلى ٢,٠٠٠,٠٠٠

(19) http://blogs.rsa.com/anatomy-of-an-attack/

(20) http://jeffreycarr.blogspot.com/2011/06/18-days-from-0day-to-8k-rsa-attack.html

زومبي لمدة ٢٤ ساعة ما يقارب من ٢٠٠ دولار[٢١]. وبشكل عام تُستخدم الزومبي لأداء ثلاثة أنواع من الأنشطة – إرسال رسائل إلكترونية غير مرغوب فيها، وإطلاق هجمات رفض الخدمة، وتنفيذ هجمات القاموس لكسر كلمات المرور. والمقالة المختصرة التالية عن أوليغ نيكولاينكو (Oleg Nikolaenko) وروبوتات الميقا دي (Mega-D botnet) تلقي مزيداً من الضوء على هذا العالم[٢٢].

روبوتات الميقا دي (Mega-D botnet)

منذ عام ٢٠١١ كانت هناك صناعة مصغرة لتركيب أحصنة طروادة (Trojan horses) على مئات الآلاف من أجهزة الحاسب الآلي، ومن ثم تأجير قدرة معالجة تلك الأجهزة على المهاجمين والمتسللين. ويُطلق على مجموعة الأجهزة المخترقة اسم (botnet). ومثال على ذلك هو وروبوتات الميقا دي (Mega-D botnet). وهي عبارة عن شبكة من نحو ٥٠٠,٠٠٠ جهاز زومبي والتي كانت المسؤولة عن إرسال أكثر من ٣٠٪ من رسائل البريد الإلكتروني المزعجة في عام ٢٠٠٨. وكان يتم تشغيل تلك الشبكة بواسطة شاب روسي يُدعى أوليغ نيكولاينكو (Oleg Nikolaenko). وفي مقابل تلك الخدمات كان يُدفع لذلك الشاب الروسي مبلغ ٤٥٩,٠٠٠ دولار من قبل لانس أتكينسون (Lance Atkinson)، وهو شخص من نيوزلندا ومُدان بتُهمة إرسال البريد الإلكتروني المزعج. وفي الرابع من شهر نوفمبر من عام ٢٠١٠ اعتقل أوليغ من قبل العملاء الفيدراليين في فندق بيلاجيو في لاس فيغاس وذلك لمخالفته قانون مكافحة الرسائل الإلكترونية المزعجة لعام ٢٠٠٣ (CAN-SPAM Act).

تحسس حزَم البيانات (Packet sniffing): وهو عبارة عن القيام باعتراض ومراقبة البيانات التي تمر عبر شبكة أجهزة الحاسب الآلي. ويُعد هذا التهديد خطراً كبيراً على الشبكات اللاسلكية لأن البيانات غير المشفرة والمرسلة عبر الشبكة يمكن قراءتها بسهولة باستخدام البرمجيات المجانية المتاحة (مثل -Wireshark) واستخدام المعدات القياسية لأجهزة الحاسب الآلي مثل الكمبيوتر المحمول. ويقوم المهاجمون بمراقبة نقاط الوصول اللاسلكية غير المشفرة في المحلات التجارية ومنشآت الأعمال بهدف سرقة بيانات اعتماد المستخدم لاستغلالها في وقت لاحق. ومن أكثر حوادث أمن المعلومات شهرة في الآونة الأخيرة هي حادثة تي جي ماكس (T.J.Maxx) والتي كانت نتيجة لسرقة كلمة المرور باستخدام تقنية تحسس رزم البيانات في إحدى نقاط الوصول اللاسلكية غير المشفرة.

---

(21) Ollman,G. “How criminals build botnets for profit,” Damballa, US Department of Defense Cybercrime Conference 2011, Atlanta, GA.

(22) https://en.wikipedia.org/wiki/Oleg_Nikolaenko

تخمين كلمات المرور: تهدف إلى الدخول على حساب مستخدم من خلال القيام المتكرر بتجريب كلمات مرور مختلفة إلى أن يتم العثور على كلمة المرور الصحيحة. وتتعرض أجهزة الحاسب الآلي الحساسة لمحاولات مستمرة لتخمين كلمات المرور. ويقوم المهاجم بتجريب كلمات مرور مختلفة حتى يتم العثور على كلمة المرور الصحيحة. وهذا الهجوم هو السائد بسبب أن معظم النظم تتجاهل محاولات الدخول الفاشلة المتكررة والتي تنشأ في تتابع سريع من نفس الجهاز. ومع ذلك فإن مسؤول النظام في بعض الأحيان قد يُهمل الحماية اللازمة مما يؤدي لحدوث اختراق. على سبيل المثال، قام طالب عمره ١٨ عاماً في أوائل عام ٢٠٠٩ بتشغيل برنامج لتخمين كلمات المرور طوال الليل واكتشف أن اسم المستخدم لمسؤول النظام في تويتر هو «Crystal» وكلمة المرور«happiness»[٢٣] . وسنناقش لاحقاً في هذا الكتاب تهديدات أخرى تتعلق بكلمات المرور.

في المثال أعلاه يكون النظام عادة على علم بأنه من غير المألوف للمستخدم أن يقوم بتجريب كلمات مرور مختلفة مثلاً بمعدل كلمة مرور جديدة كل ثانية لمدة ٨ إلى ١٠ ساعات. وعند اكتشاف ذلك يقوم النظام بحظر ذلك المستخدم. وهذه أحد الضوابط التقنية التي سنناقشها في القسم التالي.

الهندسة الاجتماعية (social engineering): وهي فن التلاعب بالناس بهدف تنفيذ المهام المطلوبة. وتستغل الهندسة الاجتماعية رغبة الانسان في فعل الخير وغريزة الانسان الطبيعية في الثقة. وكلما أصبحت التقنية أكثر أمناً أصبحت الهندسة الاجتماعية أكثر أهمية لوصول المهاجمين إلى الأنظمة المرغوب فيها.

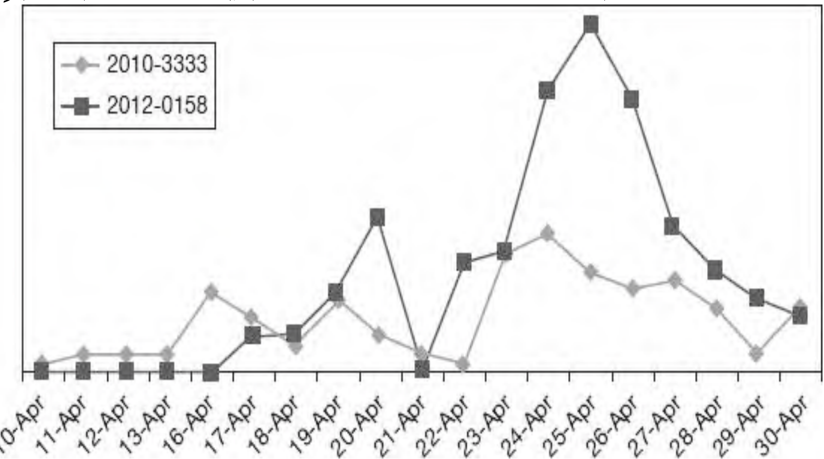
وتُستخدم الهندسة الاجتماعية عادة لبدء هجمات أخرى. وتتمثل الآلية العامة للهندسة الاجتماعية منذ عام ٢٠١٠ في إرسال رسالة إلكترونية مخصصة لمجموعة صغيرة من الضحايا الغافلين. ويكون هؤلاء الضحايا عادة في مستويات متواضعة من التسلسل الهرمي في المنظمة. وتحتوي رسائل البريد الإلكتروني على مرفقات خبيثة تتضمن الاستغلال الفوري (zero-day exploits). وعندما يقوم أي مستخدم بفتح المرفقات يتم تثبيت برنامج لتدقيق جهاز الضحية. ويقوم هذا البرنامج بتمرير المعلومات إلى المُتحكِم عن بعد، كما

(23) http://www.theregister.co.uk/2009/01/07/twitter_hack_explained/

يمكن للبرنامج أن يســتجيب للأوامر الواردة من المُتحكِم. وقد اعتمدت الهجمات المرتبطة بشركة (RSA) والتي تمت في شهر مارس من عام ٢٠١١ على منهجية الهندسة الاجتماعية.



الشكل (٤-٧): تكرار استخدام ثغرتين من الثغرات الشائعة الاستخدام في التهديد المتقدم الدائم (APT)



التهديــد المتقــدم الدائــم (Advanced persistent threat): وهــو هجــوم بشري متواصــل ومكثف يتم من خلاله رفع القدرات الكاملة لتقنيات التســلل لأجهزة الحاســب الآلي. ويهــدف تصميم هــذا النوع من التهديد لاختراق المنظــمات حتى لو كانت محمية بضوابط أمن معلومات مصممة ومصانة بشكل جيد. ولهذا السبب يتطلب هذا النوع من التهديد درجة عالية من التخصيص حســب الهدف. مــما يعني أن مجموعة ممولة تمويلاً جيداً من المهاجمين مســؤولة عن هذا التهديد. وبســبب اختلاف التهديدات التي تندرج تحت هذا النوع فإن مصطلح (APT) يشير عادة إلى فريق الهجوم بدلاً من الهجوم نفسه. والهدف العام لهذا النوع من التهديد هو استخدام الهجوم للحصول على موطئ قدم داخل المنظمة والمحافظة عليه من أجل الاستخدام والمراقبة المستمرة.

ويوضح الشــكل (٤-٧) تكرار اســتخدام ثغرتين من الثغرات الشائعة في هذا النوع من التهديد وذلك في شهر إبريل من عام ٢٠١١. وكلا الثغرتين موجود في برنامج محرر النصوص (MS Word) مما يســلط الضوء على خطورة الثغرات في البرمجيات الشــائعة الاستخدام. فالثغرة المكتشــفة في عام ٢٠١٠ تم الاستمرار في استخدامها لمدة عام من بدء الإعلان عنها،

مما يدل على تعلق المهاجمين لاستغلال الثغرات المُجربة، ويدل كذلك على الإهمال الواسع في تطبيق التحديثات. ويوضح الشكل (٤-٧) أيضاً الاعتماد السريع للثغرات الجديدة مما يشير إلى ضرورة التطبيق السريع للتحديثات[٢٤].

الضوابط:

ضوابط أمن المعلومات هي الضمانات المستخدمة للتقليل من تأثير تهديدات أمن المعلومات. وفي أنظمة تقنية المعلومات الحديثة فإن تطبيق الضوابط المناسبة والفعالة من حيث التكلفة هي واحدة من أهم مهام مسؤول النظام. وما تبقى من هذا الكتاب مخصص لشرح مختلف الضوابط واستخداماتها. ويقدم هذا الجزء لمحة سريعة عن الضوابط المختلفة.

وكما في حالة تصنيف التهديدات هناك العديد من الطرق لتصنيف الضوابط المتوفرة، وأحد طرق التصنيف الشائعة في الصناعة هي تصنيف الضوابط إلى مادية وإجرائية وتقنية.

الضوابط المادية: وهي عبارة عن استخدام الأساليب التقليدية غير التقنية لمنع الضرر. وإنها تستخدم عادة لمنع المستخدمين غير المصرح لهم من القدرة على دخول المرافق التقنية. ومن الأمثلة على تلك الضوابط: الأقفال، طفايات الحريق، والتحقق من حسن سيرة المتقدمين لوظائف المنظمة، والأبواب.

الضوابط الإجرائية: وهي عبارة عن خطط محددة للإجراءات التي تتحكم في استخدام موارد أجهزة الحاسب الآلي. وتتبع الضوابط الإجرائية لاثنين من المبادئ الراسخة لأمن المعلومات:

١. فرض المساءلة الشخصية: عندما يعرف الناس أنهم مسؤولون عن أفعالهم وأنه بالإمكان إرجاع كل فعل إلى الشخص الذي ارتكبه فإنهم يكونون بشكل عام أكثر حذراً في كل ما يختص بأفعالهم.

٢. استلزام التعاون بين أكثر من شخص للقيام بالاحتيال: «عندما يسقط اللصوص يحصل الأشخاص الأبرياء على مستحقاتهم»[٢٥]. وتشير الخبرة عادة إلى أن هناك تداعيات حول غنائم الجريمة، ويمكن للضوابط الإجرائية الصحيحة تعزيز الأمن من

(24)http://blog.trendmicro.com/trendlabs-security-intelligence/snapshot-of-exploit-documents-for-april-2012/

(٢٥) المثل كاملاً هو «عندما يسقط اللصوص يحصل الأشخاص الأبرياء على مستحقاتهم، لكن عندما يسقط الأشخاص الأبرياء يحصل المحامون على أتعابهم»، https://en.wikipedia.org/wiki/Lying_Jim_Townsend

خلال الاستفادة من نقطة الضعف البشرية تلك. ويتبع هذا المبدأ لمنطق إدارة السجلات على أساس القيد المزدوج والخاص بالإجراء المحاسبي القياسي.

ومن الأمثلة على الضوابط الإجرائية: إجراءات الحصول على حساب الكمبيوتر، وإجراءات رفع الميزات، وإجراءات تعديل البرمجيات، وإجراءات التوظيف، وضرورة إلزام المستخدمين بتغيير كلمات المرور بشكل دوري.

> كلما ازداد حجم المنظمات وكلما ازداد أمن تقنية المعلومات الأساسية، فإن التحدي الأساسي لأمن المعلومات يكمن في التأكد من القضاء على أهم نقاط الضعف في المنظمة. وأفضل وسيلة للقيام بذلك تطوير إجراءات فعالة وتطبيق تلك الإجراءات باستمرار. وكقاعدة يومية فإن خبراء أمن المعلومات يركزون بشكل كبير على الضوابط الإجرائية.

الضوابط التقنية: وهي عبارة عن الإجراءات الأمنية المبنية في نظم المعلومات نفسها. ومن الأمثلة الشائعة: كلمات المرور، والجُدُر النارية، وأنظمة كشف التسلل، وتحديث النظام، وبرمجيات مكافحة الفيروسات. ويركز بقية هذا الكتاب بشكل كبير على تفاصيل هذه الضوابط التقنية.

> ومعظم ضوابط أمن المعلومات تندرج تحت أكثر من تصنيف. على سبيل المثال، يمكن النظر إلى كلمات المرور بأنها إما ضوابط إجرائية (إجراء للوصول إلى الموارد) أو ضوابط تقنية (ضوابط مبنية في تقنية المعلومات نفسها). وفي الصناعات الحساسة (كالبنوك) يُطلب من معظم الموظفين المرور بإجراءات واسعة للتحقق من حسن سيرتهم وانضباط سلوكهم. ويمكن اعتبار هذا التحقق إما ضابطاً مادياً (غير تقني ومصمم للتحكم في الوصول المادي) أو ضابطاً إجرائياً (إجراءات متبعة للتحكم في الوصول).
>
> وهذه واحدة من نقاط ضعف طرق التصنيف في نطاق أمن المعلومات حيث يمكن بسهولة تصنيف العديد من الضوابط تحت تصنيفات متعددة.

نموذج حالة - فيروس (ILOVEYOU):

في الخامس من شهر مايو من عام ٢٠٠٠ تلقى العديد من مستخدمي البريد الإلكتروني رسائل غريبة من أشخاص يعرفونهم بعنوان «ILOVEYOU»، وقد احتوت تلك الرسائل

الإلكترونية على فيروس. وعندما يقوم المســتخدم بفتح الرسالة الإلكترونية، يقوم الفيروس بإتلاف ملفات الصور على القرص الصلب، كما يقوم بإرســال نفســه على شكل رسالة بريد إلكتروني إلى المســتخدمين الموجودين في قائمة اتصال جهــاز الضحية. وبالنظر إلى موضوع رســالة البريــد الإلكتروني المثير للاهتــمام، عُرفت تلك الرســائل الإلكترونيــة في مجال أمن المعلومات بفيروس «جرثومة الحب». وقد أصاب هذا الفايروس ما يقارب ٥٠ مليون جهاز حاسب آلي في جميع أنحاء العالم.

وكانت المتابعــة القانونية لهذا الفيروس مثيرة للاهتمام لأنهــا أظهرت القيود المفروضة عــلى إنفــاذ القانون في التعامل مع جرائم الإنترنت. وتمكــن مكتب التحقيق الفيدرالي من تحديــد مانيلا عاصمة الفلبين عــلى أنها مصدر الفيروس. كما تــم معرفة مصمم الفيروس وهــو طالب جامعي جديــد يُدعى أونيل دي جوزمــان (Onel de Guzman). لكن نشر الفــيروس لا يعــد جريمة في الفلبين في ذلك الوقت، ولذلــك لا يمكن لـ (أونيل دي جوزمان) أن يُحاكم في الفلبين، كما لا يمكن تسليمه إلى الولايات المتحدة الأمريكية لمحاكمته بموجب القوانين الأمريكية لنشر الفايروســات. وفي شــهر يونيو من عام ٢٠٠٠ وتحت ضغط دولي كثيــف اتُّهم (أونيل دي جوزمان) بجريمة الاحتيال وسرقــة بطاقات الدفع الائتمانية. لكن تم إســقاط جميع التهم لعدم كفاية الأدلة وذلك في الواحد والعشرين من شــهر أغسطس من عام ٢٠٠٠.

وفي نهايــة المطــاف أصدرت الفلبين قانوناً يُجرّم نشر الفايروســات، لكــن ذلك القانون ضعيف نســبياً لأن العقوبة القصوى هي الســجن لمدة أسبوعين وغرامة تعادل ١٠٠ دولار أمريكي.

المراجع:

Arnold, W. "Philippines to drop charges on e-mail virus," New York Times,August 22, 2000

Brenner, S.W. "Cybercrime jurisdiction," Crime. Law and Social Change, 2006, 46: 189206-

الملخص:

يصف هذا الفصل البيئة الأساسية لأمن المعلومات، كما يقوم هذا الفصل بشرح مكونات بيئة أمن المعلومــات الأربعة: الأصول المعلوماتية، وثغرات النظم، والتهديدات، والضوابط الأمنيــة. وأظهــرت الأمثلة البارزة في تلك المكونات الأربع القضايــا المُحتمل أن تواجهها في مستقبلك الوظيفي.

في هذا الفصل وفي الفصول السابقة تم تعريفك بالقضايا الهامة التي تواجهها المنظمات ومســؤولو الأنظمة. كما تم تعريفك ببعض المهارات التقنية الأساســية لأداء المهام الشائعة في إدارة الأنظمة. وتركز الفصول المتبقية من هذا الكتاب على مساعدتك في الاستفادة من تلك المهارات التقنية في تطبيق الضوابط التقنية الشائعة.

أسئلة مراجعة للفصل:

١. اشرح بشكل مختصر النموذج الأساسي لأمن المعلومات الموضح في الشكل (٤-١).

٢. ما الأصول المعلوماتية؟ أعط بعض الأمثلة من حياتك الشــخصية (يكفي ذكر بعض تصنيفات الأصول، ومن فضلك لا تنتهك خصوصيتك الشخصية عند الإجابة عن هذا السؤال).

٣. مــا هي بعض الفروق المهمة بــين الأصول التقليدية (كالذهــب، والعقار) والأصول المعلوماتية؟ وكيف تؤثر تلك الفروق في أمن المعلومات؟

٤. ما الثغرات الأمنية؟ اذكر بعضاً من الثغرات للأصول التي جرى تحديدها في ســؤال رقم ٢.

٥. ما قاعدة البيانــات الوطنية للثغــرات (National Vulnerabilities Database)؟ ولماذا هي مفيدة؟

٦. ما أحدث ثغرة أمنية تم تسجيلها بواسطة قاعدة البيانات الوطنية للثغرات؟ (وللإجابة عن هذه السؤال قم بزيارة الموقع الإلكتروني لقاعدة بيانات الثغرات الوطنية -http://nvd.nist.gov- وانقــر على وصلة محرك بحث الثغــرات -vulnerability search

engine-ومــن ثم انقر على بحث - search - وذلك باســتخدام القيم الافتراضية في جميع الحقول).

٧. ما التهديدات؟ اذكر بعضاً من التهديدات للأصول التي تم تحديدها في سؤال رقم ٢.

٨. قــم بزيارة موقع مؤشر التهديدات (أطلس-ATLAS) على الرابط atlas.arbor.net وفقاً لتاريخ (٢٠١٢/٢١/٠٥) ما الهجمة الكبرى في يوم زيارتك؟

٩. مــا الضوابط؟ وما الضوابط الهامة التي يمكنــك تطبيقها لتقليل تأثير التهديدات في السؤال السابق؟

١٠.اشرح باختصار ثغرة (عدم التحقق من صحة المدخلات). ولماذا تُعد هذه الثغرة خطرة؟

١١.اشرح باختصــار ثغرة (رفع الملفات غير المقيد). وما الأضرار التي يمكن أن تســببها هذه الثغرة؟

١٢.اشرح باختصار ثغرة (تجاوز سعة المخزن المؤقت).

١٣.اشرح باختصار ثغرة (الأذونات الناقصة). وما الصناعات التي تكون فيها هذه الثغرة بالتحديد خطرة؟

١٤.ما الثغرات الإجرائية؟

١٥.ما التوصيات لإنشاء كلمات مرور جيدة؟

١٦.ما الفيروسات والدودة الحاسوبية؟ وما الفرق الأساسي بينهما؟

١٧.قدم ملخصاً موجزاً عن فيروس (ILOVEYOU) وآثاره.

١٨.ما الانتحال (Phishing)؟

١٩.ما البرمجيات الخبيثة (Malware)؟

٢٠.ما تقنية التحكم الخفي في جهاز الحاسب الآلي (rootkits)؟ ولماذا تُعد هذه التقنية خطيرة؟

٢١.ما الزومبي؟ وفيم يتم استخدامها عادة؟

٢٢.ما الهندسة الاجتماعية؟ ولماذا تُعد تهديداً متزايد الأهمية؟

٢٣.ما الضوابط المادية؟ ولماذا تُعد هذه الضوابط مهمة؟

٢٤.ما الضوابط الإجرائية؟ ولماذا تُعد هذه الضوابط مهمة؟

٢٥.ما الضوابط التقنية؟ ولماذا تُعد هذه الضوابط مهمة؟

أسئلة على نموذج الحالة:

١. ما دافع (دي جوزمان) وراء إطلاق فيروس (ILOVEYOU)؟

٢. ما عقوبة إنشاء و/أو نشر فيروس في بلدك؟

٣. عادة تعطي القوانين للقضاة نوعاً من الحرية في تحديد العقوبات بناءً على وقائع القضية. اعتماداً على إجابتك عن سؤال رقم ٢ أعلاه، ما العقوبة التي ستحددها لـ (دي جوزمان)؟

٤. لماذا اخترت تلك العقوبة؟

نشاط التدريب العملي - أمن خادم الشبكة:

في محاولة لإعادة تصميم الموقع الإلكتروني لجامعة ولاية الشمس المشرقة، تم تطوير تطبيق للبحث في دليل الموقع. ويسمح هذا التطبيق بالبحث عن أسماء طلاب الجامعة وأعضاء هيئة التدريس والموظفين وكذلك عناوين بريدهم الإلكتروني. وقبل إطلاق موقع الجامعة، طُلب منك العمل مع فريق لتقييم أمن الموقع.

باستخدام آلة لينكس الافتراضية التي قمت بضبطها في الفصل الثاني، افتح متصفح الإنترنت من خلال النقر على أيقونة فايرفوكس (Firefox) في الشريط الموجود أعلى الشاشة (الشكل ٤-٨).

في شريط العنوان أدخل العنوان التالي: /http://www.sunshine.edu

في حقل (الاسم الأول) اكتب (william) ومن ثم انقر على إرسال (Submit)

انقر على زر الرجوع (Back) للرجوع إلى شاشة البحث

اكتب ما يلي في حقل (الاسم الأول):

william!' OR 'a'='a

أسئلة على نشاط التدريب العملي:

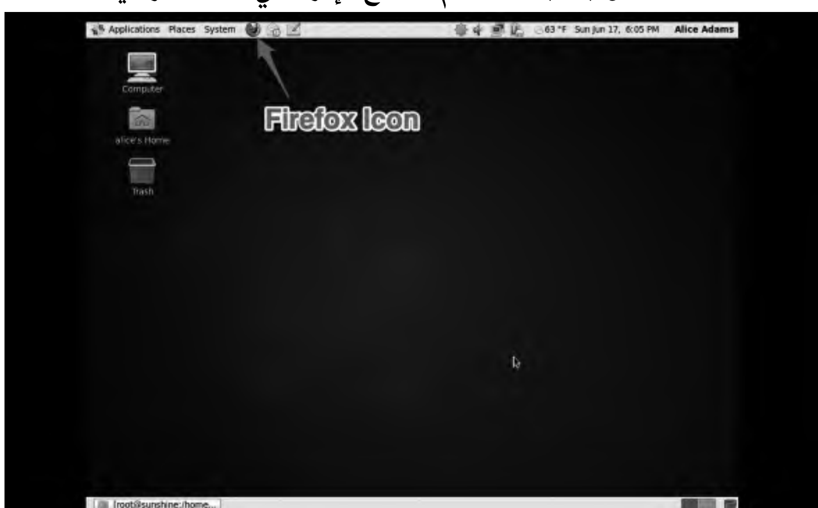
١. كم عدد نتائج البحث التي تم العثور عليها في البحث الأول؟

٢. هل حصلت على المزيد من نتائج البحث بعد تغييرك للمدخلات؟

٣. اكتـــب باختصار (فقرة إلى فقرتين) ملخصاً للنتيجة التي وصلت إليها والتي ســيتم عرضها على إدارة جامعة ولاية الشمس المشرقة. تأكد من احتواء الملخص على:

- ما الثغرة أو الثغرات التي يعاني منها هذا التطبيق؟
- ما الأسباب التي تُشعرك بوجود الثغرات؟
- ما الأضرار المحتملة لتلك الثغرات؟

الشكل (٤-٨): استخدام متصفح الإنترنت في الآلة الافتراضية



تمرين التفكير النقدي-الإنترنت، و«القيم الأمريكية»، والأمن:

تبعاً للتفكير التقليدي فإن أكبر أسـباب مشـكلات أمن المعلومـات تعود إلى عدم قيام مصممي الإنترنت ببناء الأمن في التقنيات الأساسـية للإنترنت مثل بروتوكول التحكم بالنقل (TCP)، وبروتوكـول الإنترنت (IP). فعند احتواء تلك التقنيات على الأمن سـيكون لدينا بنية معلوماتية تحتية أكثر أمناً.

لكـن أحد الكُتـاب في مجلـة (IEEE Security and Privacy magazine)، وهو دان قـير (Dan Geer) والذي يعمل مسـؤولاً تنفيذياً لأمن المعلومـات في شركة (In-Q-Tel)، وهي شركة غير ربحية تستثمر رأس مالها في التكنولوجيا وتدعم وكالة الاستخبارات المركزية (CIA)، أكد أن مصممي الإنترنت رسـخوا تفسيرهم «للقيم الأمريكية» في تقنيات الإنترنت الأساسية. وهذا هو السبب في كون برتوكول الإنترنت (IP)، وهي التقنية المسؤولة عن نقل البيانات عـبر الإنترنت، «مفتوحاً، وغير هرمي، ومُنظماً ذاتيـاً». وبمجرد أن تغادر البيانات جهازك الشـخصي، لا يكون لديك أي وسـيلة للتحكم في كيفية تسـليمها للجهة المستقبلة. وبالنسـبة لحكومـات الدول، لا يوفـر بروتوكول الإنترنت أي آلية لفـرض قيود على تدفق المعلومات من خلال الإنترنت باسـتثناء تقييد وصول المسـتخدمين للإنترنت. ويشـير دان قـير (Dan Geer) إلى أن الإنترنت قد تصبح مصدراً ناجحاً جداً لتصدير الثقافة الأمريكية، ومـن ثم يكون الإنترنت قادراً على إحداث الانفتاح وحريـة الحصول على المعلومات أينما تم اعتمادها.

واعتـماداً على وجهة النظـر تلك فإن دان قـير (Dan Geer) يعتقد أن نقص الأمن في التقنيات الأساسية للإنترنت يُعد مصدراً للقوة وليس مصدراً للضعف. فالإنترنت تتطلب من المستخدم النهائي تحمل مسؤولية الأمن الخاص به بدلاً من الاعتماد على الأمن الذي توفره بُنية الإنترنت. وفي الوقت الذي لا تتحمل فيه الإنترنت مسـؤولية الأمن فإنها أيضاً لا تقيد أي مسـتخدم من الاتصال بأي مستخدم آخر، ومن ثم تحمي حقوق المستخدمين في حرية الترابط. وقد تحد الإنترنت الآمنة من تلك الحرية باسم الأمن، وذلك بطلب إذن من مزود خدمة الإنترنت عند الرغبة في الوصول إلى مصادر معينة.

المراجع:

Geer, D.E. Jr. "A time for choosing," IEEE Security and Privacy, January/February 2011, 9695-

أسئلة على تمرين التفكير النقدي:

١. كيف يمكن للبنية التحتية للمعلومات أن تكون أكثر أمناً إذا تم إدخال تقنيات الأمان مثل تقنية التشفير؟

٢. كيف يمكن أن يصاب استخدام الإنترنت بالشلل إذا تم إدخال أمان أكثر للتقنيات الأساسية للإنترنت؟

٣. بناءً على إجابتك عن السؤالين السابقين، هل تتفق مع دان قير (Dan Geer) على اعتبار أمن الإنترنت من مسؤوليات المستخدم النهائي؟

تصميم حالة:

طلب قسم نظم المعلومات الإدارية في جامعة ولاية الشمس المشرقة منك أن تقوم بزيارة قصيرة للقسم. وفي الواقع هناك قلق في القسم بشأن الأمن الشامل للبيانات ويرغب القسم في الحصول على رأي مستشار خارجي بخصوص: (١) المشكلات الرئيسة الواضحة التي تم العثور عليها، و(٢) ما يمكن فعله لتقليل ظهور تلك المشكلات.

وفيما يلي بعض الأمور التي وجدتها أثناء زيارتك:

١. «غرفة الخادم» عبارة عن خزانة حراسة وفي زاويتها مصدر للطاقة المتواصلة (UPS)، وفيها أيضاً سبعة خوادم مثبتة على الرفوف.

٢. تحتوي ثلاثة من تلك الخوادم على بطاقة واحدة فقط للشبكة (network card)، وسلك الشبكة لبقية الخوادم الأربعة موصول في محول الشبكة نفسه.

٣. يبدو أن مصدر الطاقة المتواصلة (UPS) يعمل بسعة نسبتها (٨٠٪)، ويتوقع الفني أن وقت عمل مصدر الطاقة يصل إلى ٥ دقائق قبل أن يتوقف.

٤. يحتفظ العديد من الأساتذة الباحثين بخوادمهم في مكاتبهم.

٥. أخصائي الدعم الفني يستخدمون كلمة المرور الخاصة بمسؤول النظام نفسها للوصول إلى جميع الوحدات الطرفية في القسم.

اذكر ما لا يقل عن خمسة من التهديدات التي تجدها في القائمة أعلاه. بعد ذلك اقترح خمسة من الضوابط التي يمكن إضافتها للقضاء على تلك التهديدات. واحرص على أن تكون إجابتك مكتملة قدر الإمكان.



الفصل الخامس

تحديد الأصول والتعرف على خصائصها

نظرة عامة:

لقـد رأينا أن أمن المعلومـات يرتبط بالأصول المحددة إذ إن جميع الأنشـطة المتعلقة بأمن المعلومات كالضوابط الأمنية، وبرامج التعافي من الكوارث واستمرارية العمل، وتقييم المخاطـر، يجب أن ترتكز على حماية خصوصية أصـول المنظمة وتكاملها وجاهزيتها. وقد يـؤدي تحديد الأصول غير المرضي عنها إلى بقاء الأصـول الثمينة دون حماية في حين تقضي المنظمـة وقتهـا في حمايـة الأصول ذات القيمـة المنخفضة. ومن ثم فـإن تحديد الأصول وتصنيفها هو أساس برنامج أمن المعلومات.

وسـنقوم في هذا الفصل بوصف الأصول المهمة في المنظمات. كما سنقوم بدراسة كيف يمكـن تحديد هذه الأصول وتصنيفها. وسـنناقش في الفصول القادمـة كيفية حماية هذه الأصول. وفي نهاية هذا الفصل سوف:

- تكـون عـلى دراية ببعـض المشـكلات ذات العلاقـة بالمحافظة على أصـول تقنية المعلومات.
- يكون لديك فهم أساسي لرسالة المنظمة.
- تكون مدركاً لكيفية تصنيف أصول المنظمة وذلك بالمواءمة مع رسالة المنظمة.
- تكون مدركاً لقضايا إدارة الأصول بما في ذلك دورة الحياة والملكية.

مقدمة حول الأصول:

الهدف من تحديد الأصول وتصنيفها هو الجمع الاسـتباقي لجميع المعلومات الضرورية في الاسـتجابة للتهديدات التي تؤثر في أصول المنظمة. وينبغي أن يؤدي تحديد الأصول إلى نشر آليات المراقبة المطلوبة بحيث تستطيع المنظمة معرفة الهجمات، ومن ثم يمكنها اتخاذ

الإجــراءات اللازمة. وفي حال عدم وجود التحديــد والتصنيف الفعال للأصول فإن المنظمة قــد تكون غــير مدركة للمخاطر المحيطة بها. وفي الواقع يشــير التقرير المتعلق بتحقيقات اخــتراق البيانات الصادر من شركــة فيريزون (Verizon) في عــام ٢٠١٢ إلى أن (٩٢٪) من جميع حوادث أمن المعلومات تم تحديدها من قِبل طرف ثالث وذلك بعد أسابيع أو أشهر من وقوع الضرر[1]. ومن المفيد أن تقوم بنفســك بتحديــد الأصول قبل أن يقوم خصومك بتحديدها لك.

وفي الفصــل الرابــع عرّفنا الأصول بأنها الموارد أو المعلومــات التي يجب حمايتها. لكن كيــف يمكنك أن تعرف ما الذي يتوجب حمايته؟ مــا هو جدير بالحماية في منظمة ما قد لا يُعد مهماً في منظمة أخرى. على ســبيل المثال، قد تكون مجموعتك الموسيقية أحد أغلى الأصول لديك لكن صاحب العمل قد لا يهتم كثيراً لذلك. لذا فإن تحديد الأصول وتصنيفها تُعد إلى حد ما عملية فريدة لكل منظمة.

وفي حــين أنــه لا يمكن تطوير قائمة مُبســطة لتحديد الأصول، فإنــه يُمكن تطوير بعض الإجراءات للقيام بذلك. وعلى مر السنوات الماضية قام خبراء الصناعة بنشر خبراتهم الجماعية ذات العلاقة بتأمين الأصول المعلوماتية على شــكل معايير مختلفة لصناعة أمن المعلومات. أيزو ٢٧٠٠٢ (والمعروف ســابقاً باسم أيزو ١٧٧٩٩) هو معيار أمن المعلومات الذي أصدرته المنظمة الدولية للمعايير (International Organization for Standardization). وهذا المعيــار يحدد إجراءات الحفاظ على الأمن بما في ذلك توصيــات تحديد الأصول وتصنيفها. ويُعد نموذج (أهــداف التحكم للمعلومات والتقنية ذات العلاقة) (Control Objectives for Information and Related Technology) نموذجــاً مماثلاً يُســتخدم عادة من قبل مدققي الحسابات ويتناول أيضاً تصنيف أصول تقنية المعلومات. وفي هذا الفصل سنعمل على تطوير إجراءات لتحديد الأصول وتصنيفها عن طريق تجميع هذه المبادئ التوجيهية.

على مســتوى عال في المنظمة يتضمن تحديد الأصول وتصنيفها سرد جميع أصول تقنية المعلومات، وتوصيف أهمية كل أصل بالنســبة لأمــن معلومات المنظمة مع إيلاء الاهتمام لنظم تقنية المعلومات التي يعمل ضمنها كل أصل.

(1) Verizon (2012). 2012 Data breach investigations report. (p. 3)

وبشكل عام يمكن تصنيف جميع الأصول إلى نوعين: أصول عامة وأصول ذاتية. الأصول العامة هي الأصول التي توجد في معظم المنظمات، ويُعد البريد الإلكتروني مثالاً على الأصول العامة. وفعلياً تستخدم جميع المنظمات رسائل البريد الإلكتروني وسيلة أساسية للتواصل، وعملياً ستنظر تلك المنظمات لرسائل البريد الإلكتروني على أنها أصل يستحق الحماية. ويمكنك وضع قوائم لهذه الأصول العامة من دون أي معرفة خاصة بالمنظمة بناء على الخبرة السابقة والمناقشات مع الزملاء أو البحث على الإنترنت.

من جهة أخرى تُعد كشوف درجات الطلاب مثالاً على الأصول الذاتية، وذلك لأن الجامعات والمؤسسات التعليمية الأخرى تنظر إلى كشوف الدرجات على أنها أصول ضرورية يحق للخريجين طلبها في أي وقت من حياتهم. ويمكن للخريجين إقامة دعاوى قضائية في حال عدم حصولهم لفرص وظيفية نتيجة لفشل الجامعة في إصدار كشوف درجات عند طلبهم لتلك الكشوف. لكن من غير المُحتمل أن تقوم الشركات بالاهتمام كثيراً بكشوف درجات الموظفين. وباستثناء بعض الصناعات المُنظمَة (مثل الطب والمحاسبة)، فإن التدرج الوظيفي لشخص يعمل في عمل ما لبضع سنوات يعتمد على أدائه الشخصي وليس على كشف درجاته. ولذلك فإنه عندما يتم التعاقد مع الموظفين فإن أرباب العمل قد لا يهتمون بحفظ كشوف درجاتهم، ومن ثم تُعد كشوف الدرجات (أصولاً ذاتية). الأصول الذاتية هي الأصول المميزة والخاصة للمنظمة، ويتطلب التحديد السليم للأصول الذاتية في المنظمة جهداً كبيراً كما يتطلب ذلك الاهتمام بأدق التفاصيل.

وبالنسبة للموظف أو المحلل فإن تحديد الأصول الذاتية يتطلب تحديد العمليات والإجراءات والأنشطة لضمان أن المنظمة تعمل بقدرتها المثالية. ويبدأ ذلك بطرح سؤال جوهري هو: ما الذي تفعله هذه المنظمة بالضبط؟ وقد تظهر الإجابة عن هذا السؤال بسيطة جداً مثل «هذه الشركة تبيع السيارات» أو «هذا المحل يقوم بقص الشعر». لكن لتحديد جميع الأصول ذات العلاقة بالمنظمة يحتاج المحلل الأمني إلى أن يتعمق أكثر في الموضوع، وذلك لتحديد الأمور الهامة لمالكي المنظمة وعملائها وموظفيها.

تحديد الأصول الهامة للمنظمة:

وهناك نموذجان لتحديد الأصول الذاتية الهامة للمنظمة: نموذج تصاعدي (من أسـفل إلى أعلى)، ونموذج تنازلي (من أعلى إلى أسفل).

النموذج التصاعدي: التحدث مع زملاء العمل:

النموذج التصاعدي هو ما يحدث عادة عند توظيف شخص ما. كما يشار غالباً إلى هذا النمـوذج بـ «منحنى التعلم» وهي الفترة الزمنية التي يسـتغرقها الموظف الجديد للتأقلم مع عادات العمل واحتياجات المنظمة. وفي هذه الفترة إما أن يتم تسـليم الموظف الكثير من الوثائق لقراءتها وفهمها، أو أن يتم ربطه مع زملاء من ذوي الخبرة لتعليمه كيفية أداء العمـل. وتُعد هذ الفترة فرصـة مثالية للموظف الجديد لتحديـد أهمية عمليات معينة بالنسـبة للمنظمة. كما أنها فرصة للبدء في تحديد مدى ارتباط العناصر الغامضة بتحقيق أهداف المنظمة.

وفي حـين أن من المُرجح أن يكون الموظف على علـم بالموضوعات التي تجعل المنظمة ملائمـة للعملاء، يتوجب معرفة مـا هو مهم لعمليات المنظمة وربـط احتياجات المنظمة باحتياجـات العمـلاء. ولا يوجد أحد يعـرف طبيعة العمل الداخلي في المنظمة باسـتثناء الأشـخاص الذين يتعاملون مع قضايا العمل اليومية. على سـبيل المثال، يستطيع الموظف الحالي لفت انتباه الموظف الجديد إلى حقيقة أن فشـلًا بسيطاً في خادم خدمة اسم المجال (DNS server) قد يُعطّل أحد التطبيقات الضرورية لعمليات المنظمة والذي يصل سـعره لـ ٢ مليون دولار.

النموذج التنازلي: فهم أهداف المنظمة:

وبالإضافة إلى النظر إلى المنظمة من أسـفل إلى أعلى مـن خلال المحادثات مع موظفي العمليات، فإن فهم أهداف المنظمة من وجهة نظر القيادات التنفيذية هو أيضاً مهم جداً. ويمكـن القيام بذلك دون الوصول المباشر إلى القيادات التنفيذية في المنظمة. ويُعد قسـم التقارير السـنوية وقسـم «من نحن» في الموقع الإلكتروني للمنظمة من مصادر المعلومات

المهمة، إذ تستـــخدم الإدارة العليا تلك الأقســـام لتوصيل أولوياتهم الشـــخصية للعالم. كما تُعد بيانات الرؤية وبيانات الرســـالة من مصادر جمع المعلومات من أعلى إلى أســـفل حيث تُســـتخدم تلك البيانات من قبل قادة المنظمة للتعبير بوضوح عن قيم وأولويات المنظمات التي يُشرفون عليها.

بيان الرســـالة هو تعبير قصير (يُفضل أن يكون جملة واحـــدة أو جُملتين) عن خدمات المنظمة، والســـوق المســـتهدف، والميزات التنافسية. ويقوم بيان الرســـالة بإخبار أصحاب المصلحـــة (كالموظفين والعملاء والمورديـــن) عن أولويات المنظمة كما يقـــوم البيان بتذكير الفريق القيادي بالكيفية التي ســـيتم بها قياس النجـــاح في المنظمة. أما بيان الرؤية فيقوم بالإفصـــاح عن تطلعات المنظمة. كـــما يقوم بيان الرؤية بتحديد غايات المنظمة لكنه يقوم بالتحـــدث فقـــط إلى الموظفين حيث يقـــوم بإيصال قيم ومعتقدات المنظمـــة. ويمثل بيان الرؤية أساساً لتوقعات أداء الموظفين وسلوكهم في المنظمة، كما يمكن لرؤية المنظمة إيصال فلسلفة عمل المنظمة إلى العملاء، وذلك بوصف ما هو متوقع عند التعامل مع المنظمة.

ولأن بيانات الرســـالة، والتقارير السنوية، وغيرها من الوثائق تبذل جهداً واعياً من أجل تمييز المنظمة عن المنظمات المنافســـة، فإن الفحص الدقيق لتلك الوثائق يمكن أن يكشـــف عمّا هو مهم بالنسبة للمنظمة. وفي حين أن تلك البيانات توصف غالباً بأنها سامية وعامة، ينبغي بذل الجهد لمعرفة ما يعتقده قادة المنظمات بأنه مهم بشـــكل اســـتثنائي للمنظمة. وفيـــما يلي نعـــرض بعضاً من الأمثلة على حوادث أمن المعلومـــات التي حدثت مؤخراً، كما نعرض بيانات الرسالة للمنظمات المرتبطة بتلك الحوادث.

الشركة البريطانية لأنظمة الفضاء الإلكترونية (British Aerospace Electronic Systems)

وهي شركة بريطانية رائدة توفر منتجات الدفاع والأمن بدءاً من الخدمات الإلكترونية والدعم العسكري ووصولاً لمعدات الحماية والأنظمة الإلكترونية للمهام الحرجة. ووفقاً لموقع الشركة الإلكتروني[٢] فإن رسالة المنظمة هي «تحقيق نمو مستدام في حقوق المساهمين من خلال التزامنا بالأداء الشامل». وهذه الرسالة ليست ميزة خاصة للشركة. لذا انتقلنا لبيان الرؤية والتي تنص على «شركة الفضاء الأمنية العالمية الرائدة».

وستجد ما يلي مدرجاً في التقرير السنوي ضمن الإجراءات الإستراتيجية[٣]:

- تحسين الربحية وتطوير القدرة على توليد السيولة.
- نمو أعمال الأمن والذكاء السايبري (الإلكتروني).
- نمو الأنظمة الإلكترونية.
- تحفيز القيمة من أوضاع المنصات والخدمات.
- زيادة أعمالنا الدولية.

وتشير هذه التصريحات إلى أن الأمن والذكاء السايبري والأنظمة الإلكترونية هي الأعمال الأساسية للمنظمة. ومن المرجح أن تكون البيانات في هذه المجالات ذاتية بالنسبة للشركة. وفي الواقع كانت الشركة في عام ٢٠٠٧ ضحية لأحد الأخطار المتقدمة المستمرة (Advanced Persistent Threat)[٤]. وهي عبارة عن اختراقات متطورة للغاية تظل مخفية في شبكة المنظمة وتقوم بتسريب المعلومات للقراصنة الخارجيين. ويتم عادة نشرها من قبل الوكالات الحكومية وذلك للتجسس على التطورات التكنولوجية في الدول الأخرى. كما تم استخدامها لسرقة وثائق التصميم المتعلقة بالطائرات المقاتلة من طراز (F-٣٥) حيث كانت شركة (BAE) هي الشركة المتعهدة المسؤولة عن تلك التصاميم. ويبدو أن تلك التصاميم المسربة من شركة (BAE) قد ساعدت الحكومة الصينية في تطوير مقاتلة من طراز (J-٢٠) والموضحة في الشكل (٥-١).

(2) http://www.baesystems.com/en/our-company/about-us/our-culture

(3) التقرير السنوي للشركة البريطانية لأنظمة الفضاء الإلكترونية، www.baesystems.com/cs/groups/public/documents/document/mdaw/mdu2redisp/baes_045566.pdf

(4) After latest F-35 hack, Lockheed Martin, BAe Systems, Elbit under multiple cyber attacks….right now, https://theaviationist.com/2012/03/14/f35-anonymous-attack/

شركة ياهو

تأسست شركة ياهو في عام ١٩٩٤ من قبل طالبي دكتوراه في جامعة ستانفورد وهما ديفيد فيلو (David Filo) وجيري يانغ (Jerry Yang). ومنذ ذلك الحين تطورت الشركة لتصبح أحد شعارات الإنترنت الكبرى التي تقدم خدمات البحث والمحتوى العمودي وغيرها من الخدمات الشبكية الأخرى. وفي السنوات القليلة الماضية أصبحت الشركة تكافح على المنافسة في سوق تسيطر عليه الشركات العملاقة مثل جوجل ومايكروسوفت. وفي شهر يناير من عام ٢٠١٢ جلبت الشركة رئيساً تنفيذياً جديداً لمحاولة «إشعال الابتكار ودفع عجلة النمو». وبعد ستة أشهر فقط من العمل غيرت ياهو الاتجاه مرة أخرى وذلك بجلب ماريسا ماير (Marissa Mayer) الموظفة رقم ٢٠ سابقاً في جوجل.

وفقاً للمعلومات المتاحة للمساهمين في الموقع الإلكتروني للشركة[٥] تنص رسالة الشركة على أن «ياهو شركة الوسائط الرقمية الرائدة». أما رؤية الشركة فتنص على أن «ياهو تُحدث تجارب رقمية شخصية عميقة، وهي تُبقي أكثر من مليار شخص متصلاً بما هو مهم بالنسبة لهم عبر الأجهزة وفي جميع أنحاء العالم. وبذلك نقدم لك الطريقة التي تناسب عالمك وأسلوبك. والدمج المميز الذي تقوم به شركة ياهو بين العلم والفن والمقياس يربط بين المعلنين والعملاء الذين يبنون أعمالهم».

وفي حين أن هذه البيانات (بيانات الرؤية والرسالة) تبدو بأنها عامة فإنها تشير إلى أن ملامح الشركة الذاتية ستشمل معرفة تفضيلات المستخدمين والذين يمثلون حصة كبيرة من مستخدمي الإنترنت في العالم مما يجعلها هدفاً مرغوباً فيه للمهاجمين لمحاولة الحصول على بيانات اعتماد المستخدمين. وفي شهر يوليو من عام ٢٠١٢ حدثت زلة بسيطة في تصميم أحد خدمات الشركة، وهي خدمة صوت ياهو (Yahoo Voice)، مما أدى إلى تسرب ما يقارب من ٤٠٠ ألف من بيانات اعتماد العملاء من خوادم ياهو [٦].

الشكل (٥-١): مقاتلة من طراز (J-٢٠)



(5) Yahoo Investor FAQ, http://yhoo.client.shareholder.com/faq.cfm

(6) How The Yahoo Voices Breach Went Down, http://blog.imperva.com/2012/07/how-the-yahoo-voices-breach-went-down.html

جامعة نبراسكا – لينكولن (University of Nebraska - Lincoln)

في عام ١٨٦٩ كانت جامعة (نبراسكا – لينكولن) جامعة مُستأجرة، أما اليوم فتُعد هذه الجامعة واحدة من المؤسسات التعليمية الرائدة في البلاد، كما تُعد جامعة رائدة في البحوث لتبنيها مجموعة واسعة من المشروعات البحثية الممولة من المنح والتي تهدف إلى توسيع المعرفة في مجال العلوم التطبيقية والعلوم الإنسانية. وفي خريف عام ٢٠١١ بلغ عدد الطلاب والطالبات الملتحقين بها ما يقارب ٢٥ ألفاً. ووفقاً لموقع الجامعة الإلكتروني فإن المهام الثلاث الرئيسية للجامعة هي التدريس والبحوث والخدمة الاجتماعية. كما يحدد الموقع الإلكتروني القيم التالية للجامعة(٧):

- تعليم يهيئ الطلاب لنجاح الحياة ويهيئهم للقيادة.
- السعي للتميز دون تهاون، والإنجاز بدعم البيئة التي تحتفل بنجاح كل شخص.
- تنوع الأفكار والأشخاص.
- المشاركة مع المؤسسات الأكاديمية، والأعمال التجارية، والمجتمعات المدنية في جميع أنحاء ولاية نبراسكا والعالم.
- البحوث والأنشطة الإبداعية التي تثري التدريس، وتعزز الاكتشاف، وتسهم في الازدهار الاقتصادي وجودة حياتنا.
- إدارة الموارد البشرية والمادية والمالية المودعة تحت رعايتنا.

ومرة أخرى فإن هذه البيانات تبدو بأنها عامة نسبياً للجامعة. لكنها تُشير إلى أن معظم المعلومات الذاتية التي في حوزة الجامعة هي المواد الدراسية ومعلومات الطالب. وفقدان تلك المعلومات قد يضر الجامعة. وفي شهر مايو من عام ٢٠١٢ أدى خرق نظام معلومات الطلاب في الجامعة(٨) إلى تسريب محتمل للمعلومات الشخصية لـ ٦٥٤ ألف طالب بما في ذلك أرقام الضمان الاجتماعي. ويتجاوز العدد (٦٥٤ ألفاً) بشكل كبير عدد الطلاب الملتحقين بالجامعة لأن الجامعة تحتفظ بسجلات لجميع الخريجين. وبالإضافة إلى ذلك فإن العديد من الجامعات تحتفظ على الأقل ببعض المعلومات الخاصة بجميع المتقدمين للجامعة. وعلاوة على ذلك فإن بعض الجامعات تجذب أيضاً أعداداً كبيرة من الطلاب من خلال البرامج غير الأكاديمية مثل البرامج الإثرائية الصيفية.

ويظهر من هذه الأمثلة أن من المرجح أن تكون تلك المنظمات مُستهدفة للحصول على المعلومــات الذاتية التــي في حوزتها. ومن خلال فحص المبــادئ التوجيهية للمنظمة يمكن تحديد مثل هذه المعلومات على الرغم من أن هذا الفحص ليس طريقة علمية دقيقة.

(7) http://www.unl.edu/about-unl/role-mission/

(8) http://nebraska.edu/security

أنواع الأصول:

أثناء قيامك بتحديد الأصول في منظمتك فإنه من المفيد معرفة ما الذي تبحث عنه. ما الأنــواع المختلفة للأصول في المنظمة؟ وفي حين أن بعض المنظمات لديها أصول فريدة جداً فإن أهم الأصول التي من المحتمل أن تواجهها في أمن المعلومات هي الأصول التالية، هذه الأصول موجودة في جميع المنظمات بشكل أو بآخر وسوف ننظر في كل منها فيما يلي:

- الأصول المعلوماتية.
- الأصول الوظيفية.
- أصول مكونات الحاسب الآلي المادية.
- الأصول البرمجية.
- الأصول القانونية.

الأصول المعلوماتية:

الأصــول المعلوماتية هي المحتوى الإلكتروني المحفوظ والمملوك من قبل فرد أو منظمة. وفي الغالــب تكون هذه الأصــول أهم الأصول في المنظمة من وجهــة نظر أمن المعلومات. وتنطــوي جميع هجمات أمن المعلومــات المتعمدة على المنظمات عــلى محاولات لسرقة البيانــات. وتُعد الحوادث التي تؤدي إلى فقدان البيانات الأكثر إيلاماً (مثل تحطم الأقراص الصلبــة) عــلى أمن المعلومات. لذلك فــإن عنصراً هاماً من عناصر تحديد الأصول يشــمل البحث عن البيانات والمعلومات الهامة للمنظمة.

وتشــمل الأصــول المعلوماتية الملفات الفردية كالصور والفيديــو والملفات النصية. كما تشــمل المحتويات الرقمية الأخرى مثل البيانات الموجودة في قواعد البيانات. وتكون تلك الأصــول مخزنة إما على أجهزة مملوكة للمنظمة (محلياً) أو على أجهزة يمكن الوصول إليها في الســحابة الإلكترونية، وذلــك في كثير من الأحيان كجزء مــن الخدمات المقدمة من قبل طرف ثالث ويحكمها الاتصال مع المنظمة.

وتتضمن أمثلة أصول المعلومات العامة ما يلي: بيانات الرواتب، وبيانات التدفق النقدي، وبيانات تواصل العملاء، ومعلومات بطاقات الدفع الائتمانية، والحسابات الدائنة، وحسابات القبض، وعوائد الضرائب، والبريد الإلكتروني. وبالإضافة إلى مثل تلك المعلومات الخام فإن أصول المعلومات العامة تشمل أيضاً معالجة المعلومات مثل وثائق النظام، وأدلة تدريب المستخدم، والوثائق التشغيلية التي تضمن الامتثال التنظيمي، ومعلومات استمرارية العمل.

أما أصول المعلومات الذاتية فتشمل الملكية الفكرية مثل تصميم المنتجات ونتائج اختبار المنتجات. وتشير الملكية الفكرية (intellectual property) إلى إبداعات العقل (الاختراعات والمصنفات الأدبية والفنية والرموز والأسماء والصور والتصاميم) التي يمكن استخدامها لتحقيق الأرباح[٩]. وفي سياق مثال الجامعة فإن أمثلة المعلومات الذاتية تشمل درجات الطلاب النهائية، ودرجات اختبارات الطلاب، وكشوف درجات الطلاب.

وعلى الرغم من أن البيانات منتشرة فإن القادة التنفيذين لا يهتمون إلا بالآثار الأمنية للمعلومات التي تجذب الاهتمام السلبي لوسائل الإعلام أو تلك المشمولة بمسائل الامتثال القانوني. على سبيل المثال، معظم المسؤولين التنفيذيين على بينة بالآثار الأمنية المترتبة على بيانات بطاقة الائتمان، وهذا بسبب العديد من حوادث سرقة بطاقة الائتمان التي حدثت في الماضي القريب. ونتيجة لذلك يتم مناقشة هذه القضية في جميع مجريات الصناعة. وهذا مثال مشهور للتحيز الإدراكي، والمعروف بتحيز الحداثة، حيث يدفع العقل اهتماماً غير عادي للأحداث الأخيرة.

والتحدي الذي يواجه المتخصصين في مجال الأمن هو تحديد أصول المعلومات قبل أن يُمثل فقدان تلك المعلومات ضرراً للمنظمة. تأمل في مثال (أحضر جهازك الخاص) (BYOD) الموضح أدناه.

(9) http://www.wipo.int/about-ip/en/

(أحضر جهازك الخاص) (Bring Your Own Device)

قد تكون على علم بأن أحد أبرز الاختصارات الحديثة في منظمات تقنية المعلومات هو اختصار (BYOD) الذي يعني (أحضر جهازك الخاص). وهذا انعكاس لحقيقة أن المنظمات، مع كل جدران الحماية والمعدات الأمنية الخاصة بهم، لم تكن قادرة على احتواء انتشار الأجهزة المملوكة للمستخدم والتي يمكنها الوصول إلى شبكات المنظمات، والأهم من ذلك أنه يمكنها الوصول لبيانات المنظمات. وبعد مقاومة مبدئية لتلك الأجهزة بدأت العديد من المنظمات بالترحيب بها. وأحياناً كان الدافع وراء ذلك تقليل التكاليف، فإذا تم السماح للموظفين، ولو ببعض الجهد، باستخدام أجهزتهم الشخصية لإنجاز المهام المتعلقة بالعمل فإنه يمكن للمنظمة توفير تكاليف توريد تلك الأجهزة للموظفين. على سبيل المثال، يمكن لخط الهاتف المحمول أن يكلف ١٠٠ دولار شهرياً، أو ما يقارب من ١٠٠٠ دولار لكل موظف سنوياً. وتقريباً كل ٥٠ موظفاً يستخدمون هواتفهم المحمولة الشخصية بدلاً من الهواتف الصادرة من العمل، وذلك يساعد المنظمة على توفير وظيفة مهنية واحدة برتبة مبتدئ. إذاً فإن اقتصاديات (أحضر جهازك الخاص) (BYOD) حقيقة واضحة.

ومن منظور أمني من المهم أن نلاحظ أن (BYOD) تخلق تحديات في إدارة الأصول المعلوماتية، وذلك لأن بيانات المنظمة الآن موزعة في العديد من الأجهزة الشخصية. وسرقة أي من هذه الأجهزة بالإمكان أن تؤدي إلى اختراق الأصول المعلوماتية في المنظمة.

ولهذا السبب فإن معظم المنظمات تُصر على أن تكون قادرة على المسح الكامل لـ (BYODs) عن طريق التحكم عن بعد في حالة السرقة، أو الأذى، أو أي مخاوف أخرى.

الأصول الوظيفية:

يُعد المبرمجون والمطورون والمديرون أصولاً تنظيمية مهمة. وقد يستغرق العثور على الموظف الذي يمتلك المهارات المطلوبة ويكون على استعداد للعمل بالراتب الشهري الذي تستطيع المنظمة منحه إياه وقتاً طويلاً. وبعد التعاقد مع الموظفين تستثمر المنظمة مبالغ كبيرة في تدريبهم. وحتى لو كان ذلك التدريب غير رسمي، والذي يشمل فقط طرقاً معينة مثل متابعة موظف آخر لمعرفة قضايا العمل اليومية، أو قضاء أيام في المكتب لقراءة وثائق المستخدم، فإن ذلك يشكل تكاليف إضافية للمنظمة. وفي وقت لاحق مع تطور الموظف مهنياً ومع تعلم الأساسيات وبناء شبكة اجتماعية داخل المنظمة قد يجد الموظف

نفســه خبيراً في مجال معين. على ســبيل المثال، قد يتطور الموظف ليصبح الأفضل في فهم شيء يمكن أن يكون عملية أساســية للقســم الذي يعمل فيه مثل معالجة السلسلة في لغة بيرل (Perl)، أو ضبط اللغة الاستفسـارية الإنشـائية المركبة (MySQL) لتحقيق أداء عالٍ للعمليات، أو تعظيم الاســتفادة من قواعد جدار الحمايــة. وكمحلل لأمن المعلومات فإن من أحد مسؤولياتك تحديد هؤلاء الأفراد وإدارة المخاطر المرتبطة بهؤلاء الموظفين المميزين. وإحدى الطرق لذلك هي جعل الإدارة واعية لأهمية هؤلاء الأفراد حتى تقوم الإدارة بمزيد مــن الجهود لإشراكهم في العمل. وآلية أخرى لتحقيق ذلك هي تدريب موظفين آخرين في المنظمة على مهارات متعددة للتصدي لبعض تلك المسؤوليات الهامة.

ويتم توثيق الأصول الوظيفية أيضاً من وجهة نظر الاستجابة للكوارث. فعندما يتعرض أحد الأصول لتهديد ما عليك أن تعرف كيفية الاتصال بالأفراد القادرين على الاستجابة لهذا التهديد. وتأتي هذه الوثائق على شــكل تجميع لأرقام الهواتف، وعناوين المنازل، وعناوين البريد الإلكتروني، أو أي شكل آخر من أشكال معلومات التواصل.

أصول مكونات الحاسب الآلي المادية:

وتشمل أصول مكونات الحاسب الآلي المادية قطع الآلات المادية والنظم المرتبطة بشكل مباشر أو غير مباشر في دعم رســالة المنظمة. وهي عادة ما تُمثل «الأشياء» التي تم شراؤها مــن الإيرادات، ورســوم الطلاب، والمنح النقدية وغيرها. كما تمثل مكونات الحاســب الآلي المادية الوسيط الذي توجد فيه البيانات، ومن ثم فمن دون هذه المكونات المادية لا يمكن أن يكــون هنــاك بيانات لتأمينها، وعند ذلك لا يكون هنــاك حاجة لأمن المعلومات. وتُعد مكونات الحاسب الآلي المادية أمراً بالغ الأهمية للقسم كأهمية البيانات التي تحتويها تلك المكونات.

وبالإضافة إلى الدور الموضح أعلاه بأن مكونات الحاسب الآلي المادية تمثل أصولاً للأغراض العامة، قد تكون مكونات الحاســب الآلي المادية أصلاً ذاتياً للمنظمة في شكل نموذج مبدئي لجهاز جديد، أو براءة اختراع جديدة. وتُعد النماذج المبدئية عادةً شكلاً من أشكال الملكية الفكريــة. كما تمثل النماذج المبدئية غالباً القاعدة للفرص المُســتهدفة من المنظمة ولذلك

تحمي المنظمات النماذج المبدئية بعناية فائقة. ولحماية الفرص التجارية المرتبطة بالنماذج المبدئيـــة، فإن إصدار أي معلومات متعلقة بالنماذج المبدئية يكون محمياً بواســطة عقود تُسمى باتفاقيات عدم الإفشاء (Non-Disclosure Agreements).

> وكمثال على خرق أمني يتضمن نموذجاً مبدئياً للمكونات المادية، في عام ٢٠١٠ نسي أحد موظفي شركة أبل (Apple) نموذجاً مبدئياً لهاتف أيفون (S4) في إحدى الحانات في كاليفورنيا. وتم العثور على النموذج المبدئي وبيعه بـ ٥٠٠٠ دولار لمحرري موقع (Gizmodo.com). وقام الموقع الإلكتروني بنشر القصة مفصلة مع الصور. وفي شهر أكتوبر من عام ٢٠١١ تم الحكم على الرجلين المتورطين ببيع الجهاز بسنة مع إيقاف التنفيذ والوضع تحت المراقبة، وقضاء ٤٠ ساعة في خدمة المجتمع، كما حُكم على كل منهما بدفع ٢٥٠ دولاراً تعويضاً لشركة أبل.

تتبع الخصائص:

ماذا ينبغي على المنظمة أن تُســجل لتتبع أصول مكونات الحاســب الآلي المادية؟ هذه العمليــة هي الأســاس للعديد من الأنشــطة الأمنية الأخرى بدءاً مــن التعافي من الكوارث ووصــولاً لإدارة المخاطر. وفي الوضع المثالي ترغــب أن تكون المعلومات كاملة قدر الإمكان بحيث إذا فقدتَ جهازاً معيناً تكون قادراً على استبداله بقليل من الجهد. ويوضح الجدول (٥-١) مثالاً على تتبع خصائص أجهزة الحاسب الآلي المكتبية وأجهزة الحاسب الآلي المحمولة.

ويجــب أن تلاحظ في هذه المرحلة أن الجدول في الواقع يتضمن أكثر من مجرد الوصف المادي للجهاز.

تكلفــة الشراء وتقدير نهاية حياة الجهاز: تكلفة الشراء تُعطيك معياراً عند البحث عن تكاليف التأمين والاستبدال في حال فقدان الجهاز. ستحتاج إلى قرابة ١٠٠٠ دولار لاستبدال هذا الجهاز. ويســاعدك تقدير نهاية حياة الجهاز من ناحيــة الميزانية. فيجب أن تخطط لاســتبدال هذا الكمبيوتر المحمول في نحو ٣ ســنوات. وفي ذلك الوقت ســتحتاج إلى قرابة ١٠٠٠ دولار.

تاريخ تســليم الأصول وتاريخ الإنتــاج: هذه التواريخ تعطيك لمحــة عن مدى كفاءة تقنية المعلومات وإعداد الجهاز للاســتخدام. وتشــمل تثبيت نظام التشغيل والتطبيقات،

والتهيئة، والتســليم الأخير إلى المســتخدم النهائي. وفي نهاية الســنة المالية قد تزيد الفترة الزمنية بين هذه التواريخ وذلك عندما تقوم الإدارات بتقدير مشترياتهم. وقد تُشير الزيادة غــير الطبيعيــة إلى تعقيدات إضافية في العملية أو في الحاجــة إلى مزيد من الكادر البشري المخصص لإعداد أجهزة الحاسب الآلي.

الجدول (٥-١): مثال على تتبع الخصائص

النوع	جهاز الحاسب الآلي المحمول
رقم البطاقة أو المُعرف الفريد	6000001-724872-
الشركة المنتجة	ASUS
رقم الموديل	U٤٦BAL٥
الرقم التسلسلي	-V١٢٨٣٤VJHF-BV
العنوان المادي (MAC Address)	0008--CA-8479-40-
بطاقة الخدمة (إن وجدت)	URG٦٤V
الوصف	جهاز حاسب آلي محمول ١٤ بوصة، غطاء فضي
وحدة المعالجة المركزية (CPU)	Core i7, 2.7 GHz
تكلفة الشراء	958 دولار
تاريخ الشراء/التأجير	52012/1/
تقدير نهاية حياة الجهاز	٣ سنوات
تاريخ تسليم الأصول إلى إدارة تقنية المعلومات	52012/15/
تاريخ الانتاج	52012/20/
المستخدم الأساسي	Dr. Jane Davis
الموقع	PHY Building, 475A
الخدمة الأخيرة تمت بواسطة	Elmer Livingstone
قابس الشبكة	PHY475A-B
تاريخ الخدمة	52012/16/
تاريخ التخلص من الجهاز	
سبب التخلص من الجهاز	
توجيهات خاصة للتخلص من الجهاز (الامتثال للوائح)	يحتوي جهاز الحاسب الآلي المحمول على بيانات بحثية تخضع لضوابط التصدير لذا يجب أن تُمحى فور استلامها من قبل موظفي تقنية المعلومات وفقاً للتوجيهات الإرشادية لوزارة الدفاع.

وقد تكون لاحظت أن هذه «السـيرة الذاتية للجهاز» سـتكون في الواقع مفيدة للعديد من الإدارات في تقنية المعلومات، كما ستكون هناك مجموعات مختلفة من الموظفين قادرة على المسـاهمة بالمعلومات. ويجب أن يكون موظفو الشـبكات على سبيل المثال قادرين عـلى الإفادة برقم القابس الموصـل بجهاز معين. كما يجب أيضاً أن يؤكدوا الموقع الفعلي. أما موظفو دعم الحاسـب الشـخصي فيجـب أن يكونوا قادرين عـلى تحديث آخر موعد للخدمـة، ويمكن لموظفي الامتثال للوائح من اسـتخدام التاريـخ للتوصل إلى قائمة تتضمن تواريخ آخر الفحوصات التي تمت بواسطة موظفي تقنية المعلومات.

سرقة أجهزة الحاسب الآلي المحمولة، والسيرة الذاتية للجهاز، والاتصال بالشبكة

في جامعة جنوب فلوريدا، تشارك شرطة الجامعة باستمرار بالبحث عن أجهزة الكمبيوتر المحمولة المسروقة. يذهب الطالب للمكتبة ومن ثم «يبتعد للذهاب لدورة المياه». وعند عودته لا يجد جهازه.

وعندما يُسجل الطلاب للتواصل اللاسلكي في حرم الجامعة فإننا نحافظ على السجل الذي يربط الجهاز الفعلي للمستخدم مع هويته. وعندما تتواصل شرطة الجامعة مع تقنية المعلومات فإننا نقوم بوضع أثر تعقب على الجهاز الفعلي وننتظر لنرى ما إذا كان الجهاز يظهر على الشبكة مرة أخرى.

وغالباً ما يحدث ذلك.

استكشاف الأصول:

إدارة الأصول من خلال دورة حياتها هي القاعدة الذهبية. ولكن واقعياً غالبية المنظمات، وخاصة المؤسسـات الصغيرة والمتوسـطة الحجم، ليس لديها إجراءات رسمية لمتابعة أصول (مكونات الحاسب الآلي المادية) من خلال دورة حياتها.

يتم استبدال الخوادم عندما تتعطل أو عندما تكون قديمة جداً وعندما يؤثر عدمُ قدرتها عـلى الأداء في النتائج الأساسـية للمنظمة. وفي الجامعات يتم تمرير أجهزة الحاسـب الآلي المكتبيـة من أعضاء هيئة التدريس إلى المسـاعدين الإداريين. ويتم شراء الأجهزة من المنح المالية وبطريقة سـحرية «تظهر» تلك الأجهزة على الشـبكة خلال يوم واحد. وفي معظم

الإدارات لا أحـد يعلم حقـاً (١) ما هي أصول مكونات الحاسـب الآلي المادية التي تملكها الإدارة، (٢) وأين مكان تلك الأصول.

ويمكن أن يُسـتخدم مسح الشـبكة من أجل التوصل إلى قائمة بهذه الأجهزة. وللأسف فإن مسح الشبكة ليس دقيقاً لأن الأجهزة المحمولة قد لا تكون متصلة بالشبكة خلال فترة المسح. وحتى أن المسح المتعدد، والذي يتم في أوقات مختلفة، قد لا يلتقط جميع الأجهزة. وللتعامل مع هذه القضية فإن العديد من المنظمات تتبنى سياسات تتطلب مراجعة دورية لجميع الأجهزة ويقوم بتلك المراجعة موظفون من خارج المنظمة.

معظم الشركات والجهات الحكومية لديها مبادئ توجيهية يتم من خلالها تعقب فقط الأصول التي تتجاوز مستوى معين من التكلفة. لكن تلك المبادئ التوجيهية مبنية في الغالب على أسباب مالية فقط لأن لدى محلل أمن المعلومات أسباباً تقنية لتتبع الأجهزة، على الرغم من أن تلك الأجهزة قد تكون تحت مستوى التكلفة المحدد من المنظمة.

الأصول البرمجية:

الأصـول البرمجية هـي الأدوات البرمجية اللازمـة لمعالجة معلومـات المنظمة بهدف تحقيق رسالة المنظمة. وتحتاج الأصول البرمجية للحماية من أجل ضمان أن البيانات داخل المنظمة جاهزة للاسـتخدام بحيث تتمكن المنظمة من المحافظة على مسـتويات عالية من الإنتاجية. وهذه الأصول البرمجية لها العديد من خصائص أصول (مكونات الحاسـب الآلي المادية). وتشـمل الأصول البرمجية العامة تطبيقات المستخدم مثل (Microsoft Office)، كما تشمل التطبيقات المؤسساتية مثل (PeopleSoft) (وهو يستخدم للحفاظ على بيانات الموظفـين)، وأدوات التطوير، ونظم تتبع إصدار البرمجيـات، والبرمجيات المتعلقة بالأمن. وتسـتلزم حماية الأصول البرمجية بعض الأنشـطة مثل التأكد مـن إتاحة الإصدار الأحدث مـن البرمجيات والتأكد من أن إصدارات البرمجيات المتاحة متوافقة مع الأجهزة الموزعة في المنظمة. ويتم عادة شراء الأصول البرمجية العامة.

الأصـول البرمجية الذاتية هي الأصـول التي يتم عادة تطويرهـا في المنظمة، إما لدعم العمليات الداخلية وإما للبيع بوصفه مُخرَجاً من مخرجات المنظمة.

الأصول القانونية:

الأصـول القانونيـة المتعلقة بتقنية المعلومات هـي التنظيمات التعاقديـة التي توجه اسـتخدام أصول (مكونات الحاسـب الآلي المادية) والأصول البرمجية داخل المنظمة. ومن الأمثلة عـلى تلك الأصول اتفاقيات الدعـم الفني وتراخيص البرمجيـات، ومصادر الدخل، ومصادر التمويل. وقد تُنسى هذه الأصول بسـبب مسـيرة الأعمال اليومية في المنظمة مما يـؤدي ذلك إلى حـدوث خلل. وأحد الحـوادث المعروفة والتي تدل عـلى أهمية الأصول القانونية المتعلقـة بتقنية المعلومات هي حادثة شركـة (Comair) وهي إحدى الشركات التابعة لخطوط دلتا الجوية[١٠]. ففي عام ٢٠٠٤ كانت شركة الطيران تستخدم نظاماً لجدولة طاقم الطائرة تم اقتناؤه في عام ١٩٨٦.

الجدول (٥-٢): مثال على الأصول

الأصول	نوع الأصول
جهاز حاسب آلي محمول	أصول مكونات الحاسب الآلي المادية
درجات الطلاب	أصول معلوماتية
المحلل الأمني فلان الفلاني	أصول وظيفية
حزمة برامج مايكروسوفت أوفيس	أصول برمجية
ترخيص مايكروسوفت أوفيس	أصول قانونية

وتضع أنظمة سـلامة الطيران توجيهات صارمة على سـاعات عمل طاقم الطيران، وذلك لضـمان يقظتهم ويعمل نظام جدولة طاقم الطائـرة على ضمان الامتثال لتلك التوجيهات. والنقطـة المُهملـة في الموضوع هي أن عدد تراخيص التغيـيرات التي حصلت عليها الشركة هو ٣٢ ألفاً حداً أعلى خلال أي شـهر. الشركة حصلت على تراخيص لـ ٣٢ ألف تغيير حداً أعلى خلال أي شـهر. وقد تسبب شتاء قارس وغير اعتيادي في شهر ديسمبر من عام ٢٠٠٤ وصول الشركة إلى هذا الحد لأول مرة في ليلة عيد الميلاد. وبدون البرمجيات لا يمكن لشركة الطيران أن تعمل على الرغم من أن كل طائراتها كانت تعمل بكامل طاقتها. وقد أدى هذا

(10) http://www.cio.com/article/2438920/risk-management/comair-s-christmas-disaster--bound-to-fail.html

الحادث إلى احتجاز أكثر من ٢٠٠ ألف عميل في المطارات في عيد ميلاد عام ٢٠٠٤، وخسارة قدرها ٢٠ مليون دولار (مقارنة بأرباح قدرها ٢٥ مليون دولار في الربع السـنوي السـابق)، كما أدى ذلك إلى رحيل الرئيس التنفيذي السابق للشركة. وكل ما كان مطلوباً لتجنب وقوع تلك الحادثة هو الانتباه لمسـتوى تراخيص التغيـيرات وشراء العدد المطلوب من التراخيص الإضافيـة. ومَثلت هذه الحادثـة موضوعاً لأحد الكتب الممتعة جداً في إدارة مخاطر تقنية المعلومات[11].

تحديد الأصول - مثال من جامعة نموذجية:

وبعد أن ذكرنا فيما سبق تصانيف الأصول المهمة، نستطيع الآن تحديد هذه الأصول في أي منظمة. وتُعد الأصول العامة أسـهل في التحديد، وذلك لأن قوائم الأغراض العامة يمكن صياغتها لتحديد تلك الأصول. أما الأصول الذاتية فهي محيرة أكثر لأن تحديد هذه الأصول يتطلب معرفة عميقة بالمنظمة وبالصناعة التي تعمل فيها المنظمة. ولحل هذه المشكلة في تحديد الأصول، يوصي الكثير من الخبراء بتطبيق مزيج من النموذج التصاعدي (من أسـفل إلى أعلى)، والنموذج التنازلي (من أعلى إلى أسفل). إن تحديد ما هو مهم بالنسبة للمنظمة يمكن أن يساعد في تحديد الأصول الذاتية للمنظمة. ويوضح الجدول (٥-٢) مثالاً على بعض الأصول النموذجية التي قد تجدها في إحدى الجامعات.

التعرف على خصائص الأصول:

وبعد أن قمنا بتحديد جميع الأصول مع إبراز النظام ومعرفة تبعياته، نحن مسـتعدون الآن للبـدء في التعـرف على خصائص الأصـول. وللقيام بذلك هناك معياران: الحساسـية والأهمية. ويسـاعد التعرف على خصائص الأصول على تخصيص الموارد بالشـكل المناسب من أجل حماية تلك الأصول. ويمكن أن يؤدي التعرف على خصائص الأصول غير الفعال إلى اسـتثمارات كبيرة في حماية الأصول غير المهمة، في حين تكون المنظمة معرضة للمشـكلات الشائعة.

(11) Westerman, G. and Hunter R. IT Risk: Turning Business Threats into Competitive Advantage (Hardcover). Boston, MA, Harvard Business School Press

حساسية الأصول:

تصف الحساسـية مدى الضرر الذي يحدث للمنظمة بسبب اختراق خصوصية الأصول أو انتهاك تكاملها. ويمكننا شرح الحساسية اعتماداً على المثال التالي:

> بالنظر إلى الأصول التالية، أيها تعتقد أنها أكثر حساسية؟
> - الملفات البحثية للدكتور جيمسون والموجودة على سطح المكتب الخاص باتباع التعليمات المنظمة للتعامل الدولي للأسلحة، ويرجع ذلك إلى حقيقة أن تلك الدراسات تتضمن بحوثاً عن مواد تحت رقابة القوات المسلحة الأمريكية.
> - البريد الإلكتروني لجين بولينغ وهي طالبة في كلية إدارة الأعمال.
> - المفكرة الخاصة بروبرت طومسون.

نأمـل أنك اخترت الخيار الأول. ليس لأنه أحد أعضاء هيئة التدريس بل لأنه عند تمكن شخص غير مصرح له من الوصول إلى أبحاث الدكتور جيمسون، فإن أفراد القوات المسلحة الأمريكية ليسـوا فقـط في خطر محتمل، بل يمكن أن الجامعـة تواجه عواقب وخيمة من حيث المنح. والدكتور جيمسون نفسه يمكن أن يذهب إلى السجن. وفي الواقع حدث شيء مماثل مع البروفيسـور جون ريس روث (John Reece Roth). ففي شـهر يوليو من عام ٢٠٠٩، تلقى روث حكماً بالسـجن لمدة أربع سنوات لتصديره تكنولوجيا عسكرية بطريقة غـير مشروعة ويرجـع ذلك إلى حد كبير بسـبب عمله مع طلاب دراسـات عليا من إيران والصين[١٢].

وهناك توجيهات مختلفة لتصنيف حساسية الأصول. فبعض المنظمات تستخدم مقياساً مـن صفر إلى خمسـة. والبعض الآخر يسـتخدم مقياسـاً يبدأ من (منخفـض) إلى (عالٍ). ولأغراض هذا الكتاب، سـوف نستخدم نظاماً ثنائياً بسـيطاً يصنف الأصول إلى واحدة من فئتين: مقيدة أو غير مقيدة.

(12)Prison Time and Export Controls ،http://www.governmentcontractslawblog.com/2011/10/articles/itar/

الأصول المقيدة:

الأصول المقيدة هي الأصول التي يؤدي الإفصاح عنها أو تغييرها إلى عواقب وخيمة على المنظمة. والأمر متروك للمنظمة لتقرير الحد الخاص بها. وبعض النتائج قد تكون مقبولة عند مقارنتها بالتكاليف المطلوبة لتأمين الأصول. ويُسـمى هذا التحديد بـ (قبول المخاطر) وسيتم مناقشته مرة أخرى في فصول لاحقة.

خذ درجاتك الدراسـية على سـبيل المثال. تُعد درجاتك الدراسية أصولاً مقيدة بالنسبة لجامعتك. فلا يُسمح لأحد حتى لأبويك بالاطلاع على درجاتك الدراسية دون موافقتك، وإن كان أبواك يدفعان الرسوم الدراسية بالكامل. وهذا لا يحدث بالضرورة لأن الجامعة واحدة مـن الخيـارات. فالجامعات مُلزمة بحماية درجاتك الدراسـية وغيرها مـن البيانات وفقاً لقانون الحقوق التعليمية والخصوصية للأسرة لعام ١٩٧٤ (Family Educational Rights and Privacy Act). وهـذا القانون يُعـرف بقانون (بند الإنفاق): «لا يجوز تخصيص أي أموال لأي برنامج قابل للتطبيق....» ما لم يتم تحقيق المتطلبات القانونية[١٣]. بمعنى أنه ما لم تلتـزم الجامعة بهذا القانون فإنه لن يتم تخصيص أي أموال فيدرالية إلى الجامعة (بما في ذلك المساعدات المالية للطلاب).

وسوف تجد أنه يتم اعتبار عدد غير قليل من الأصول بأنها أصول «مقيدة» بسبب نوع من الامتثال للقوانين. ومثال على ذلك الامتثال في صناعة بطاقات الدفع (Payment Card Industry)، فالتوجيهات الصادرة من البنوك لحماية معلومات البطاقات الائتمانية، وقانون إمكانية نقل التأمين الصحي والمسـاءلة (HIPPA)، وقانون ساربينز أوكسلي (Sarbanes–Oxley Act) كلها حددت معايير محاسبية جديدة أو مطورة لجميع مجالس إدارة الشركات العامة في الولايات المتحدة، والإدارة، وشركات المحاسبة العامة.

وهناك أيضاً بعض الأصول التي يمكن النظر إليها بأنها أصول «مقيدة» بسبب اختيار المنظمة.

تقارير التعرف على خصائص الأنظمة، على سبيل المثال، تحدد بدقة أنظمة المنظمة التي تُعد حساسة للعمليات. كما أن تلك التقارير قد تُظهر بعض الثغرات التي يمكن أن يستغلها

(13)Legislative History of Major FERPA Provisions ،http://www2.ed.gov/policy/gen/guid/fpco/ferpa/leg-history.html

بعض الأشــخاص للوصول إلى النظام (هل تتذكر القنوات غير المؤمنة في البريد الإلكتروني؟). لذلك ينبغي النظر إلى خصائص الأنظمة بأنها من الأصول المقيدة. ويمكن أن تشمل الأمثلة الأخرى رواتب الموظفين، وجداول الميزانية، وتقارير المراجعة الداخلية، وغيرها.

الأصول غير المقيدة:

الأصــول غير المقيدة تختلف عن تلك الأصــول التي تُصنف بأنها مقيدة. وهي البيانات التي إذا سُربت أو تم استعراضها من قبل شخص ما فإن ذلك لن يسبب مشكلة للمنظمة.

رأينا سابقاً أن درجاتك الدراسية تُصنف تحت المعلومات المقيدة. وفي المقابل فإن لدى جامعتك ما يُسمى بدليل المعلومات الذي يحتوي على المعلومات التي تخصك والتي يمكن نشرها علناً. وتُعد المعلومات التالية عادة جزءاً من دليل المعلومات ومن ثم فهي معلومات غير مقيدة:

اســم الطالب، العنوان المحلي ورقم الهاتف، العنوان الدائم ورقم الهاتف وعنوان البريد الإلكــتروني، مكان الميلاد، تخصص الدراســة، تواريخ الحضور، حالة التســجيل بدوام كامل أو جزئي، الســنة الدراســية (المرحلة)، الدرجــة (الدرجات) العلمية الحائــز عليها، الجوائز والأوسمة الحائز عليها، المؤسسات التعليمية الأخرى التي التحق بها، صورة شخصية، الطول والوزن لأعضاء الفريق الرياضيين.

وإذا كنت مندهشاً وتتســاءل عن المعلومات التي تضعها جامعتك في دليل المعلومات، عليــك بالبحــث في دليل المعلومات لمعرفة ذلك. ويتطلب مــن الجامعات أيضاً توفير آلية لتحويــل البيانات غــير المقيدة إلى بيانات مقيدة. وعادة ما يكون هناك نموذج للخصوصية يمكنك تعبئته في مكتب المُسجل والذي يسمح لك بمنع الجامعة من نشر عنوانك الشخصي على سبيل المثال.

وتُعد المعلومات المنشــورة على المواقع الإلكترونية العامــة عادة معلومات غير مقيدة. ومــن الأمثلة على ذلك الأصول المعلوماتية التســويقية، قائمة الفصول في الجامعة، الحقائق الغذائية عن الأغذية أو المشروبات.

أهمية الأصول:

أهميــة الأصــول هي مقياس لمــدى أهمية الأصل للبقــاء الحالي للمنظمــة. وعادة ما يرتبــط مســتوى الأهمية العاليــة للأصل بمدى وجــود الأصل في إطار مبــادئ الخصوصية (Confidentiality)، والتكامــل (Integrity)، والجاهزية (Availability). وفي الواقع فإن (أهمية الأصول) تسأل هذا السؤال: إلى متى يمكن لمنظمتي البقاء دون هذا الأصل؟ وكلما كان الأصــل أكثر أهمية ازدادت التدابير التــي تأخذها المنظمة من أجل التأكد من تكرارية الأصل، وأن له نسخاً احتياطية، وأنه محمي من التعطل.

وعند محاولة تحديد مستوى أهمية الأصل سوف تجد أنه إلى حد كبير يعتمد على عين الناظــر حيث تختلف الأهمية من إدارة إلى إدارة داخل المنظمة، وخصوصاً عندما ينظر إلى الأصل بأن له فوائد فقط لمنظمتهم. وبعض الأصول تخدم بوضوح المنظمة بأكملها، وغالباً ما يشــار إليها بــ أنظمة أعمال المنظمة (Enterprise Business Systems). على ســبيل المثــال، الأنظمة التــي تتعامل مع وظائف الموارد البشرية والرواتــب عادة تُعد من أنظمة أعــمال المنظمة. في البيئة الجامعيــة يعد النظام الذي يتعامل مــع درجات الطالب نظاماً أعمال المنظمة. لكن نظام البريد الإلكتروني الذي يتعامل فقط مع كلية الطب لا يعد نظاماً لأعــمال المنظمة لأنه يعمل فقط مع هذه الكليــة. غير أن هذا النظام يعد مهماً لعمليات كلية الطلب. وتُعد أنظمة أعمال المنظمة مهمة، أما غير هذه الأنظمة فلا تُعد كذلك.

> تأمل فيما يلي عند محاولة تحديد مستوى أهمية الأصول:
>
> - ما وجهة نظرك؟
> - هل سيكون الإداريون قادرين على استرداد البيانات في حال وقوع كارثة؟
> - كم من الوقت ستستغرق عملية استرداد البيانات؟
> - هل سيكون هناك تأثير في فقدان الجاهزية بما في ذلك خسران المكانة العامة للجهة؟

وهنــاك تعريفات لفئات مختلفة من الأهمية في مجال أمــن المعلومات. وأحد أنظمة التصنيف الأساسية يُصنف الأصول إلى ضروري، ومطلوب، ومؤجل.

الأصول الضرورية:

ينبغي النظر إلى الأصل بأنه ضروري إذا كان فقدان جاهزيته سيسـبب عواقب وخيمة وفوريـة للمنظمـة. وهذا يعني أن المنظمة بحاجة إلى تحديـد تعريف مصطلح «عواقب وخيمة». وسـيتم فقدان الأصول الضرورية وإن اسـتمر غيابها فترة وجيزة من الزمن. خذ على سبيل المثال عجلات السيارة. إذا كنت تقود سيارتك على الطريق السريع فإن العجلات ضروريـة. وانفجار أحدها قد يعني كارثة كبيرة بالنسـبة لـك ولبقية الركاب. ومن الأمثلة الأخرى على ذلك: نظام الشراء لبائع على شـبكة الإنترنت، والطاقة الكهربائية للمستشفى، وقوارب النجاة لسفينة التايتانيك.

وأحـد نقاط ضعف أمـن المعلومات أن الأصـول الضرورية لا تكون محمية بالشـكل الصحيح، وأن جاهزيتها تؤخذ على أنها حقيقة غير قابلة للمناقشة. وسوف نستعرض هذا الموضوع عندما نناقش التعافي من الكوارث في الفصل الحادي عشر.

الأصول المطلوبة:

يعد الأصل مطلوباً عندما يكون مهماً للمنظمة وفي الوقت نفسـه تكون المنظمة قادرة على الاستمرار في العمل لفترة من الوقت وإن كان الأصل غير موجود.

دعنا نفكر في مثال السـيارة مرة أخرى. هذا المثال سيوضح أيضاً تبعية الوقت لمستوى أهمية الأصول. وبكل وضوح تُعد العجلات ضرورية إذا كنت تقود سـيارتك على الطريق. لكن ماذا إذا رجعت إلى منزلك وفي وقت لاحق في المسـاء واكتشفت أن أحد الإطارات خالٍ مـن الهـواء؟ وفي هذا الوقت، وعلى افتراض أنه لم يكن لديك أي مكان للذهاب إليه، يمكن اعتبار العجلات أصلاً ضرورياً: إنها مهمة ولكنها ليست حرجة. ويمكن أن تكون مرة أخرى حرجة في اليوم التالي عندما يتوجب عليك الذهاب للعمل، ولكن حتى ذلك الحين سـيكون لديـك فرصة لتصحيح المشـكلة. وأحد طرق تصحيح الأمور هـي تفعيل خطة التعافي من الكوارث: احصل على رافعة، وركب الإطار الاحتياطي، وأصلح الإطار الرديء. مدة التوقف: قرابة ٢٠ دقيقة.

الأصول المؤجلة:

الأصول المؤجلة هي الأصول اللازمة للتشـغيل المثالي للمنظمة لكن فقدان جاهزيتها لا يسـبب مشـكلات كبيرة للمنظمة في الأجل القريـب. وإذا كان يمكن وصف الأصل بعبارة «حسناً في نهاية الأمر نود الحصول عليه لكن يمكن الاستغناء عنه في الوقت الراهن»، فإنك ستعرف أن هذا الأصل من الأصول المؤجلة.

هذه الأصول هي العناصر التي يمكن أن تجعل المنظمة تعمل بسلاسة وكفاءة أكبر، لكن يمكن تجديدها عند الحاجة. خذ شيئاً بسيطاً مثل قلم الحبر الذي تستخدمه في الصف. إذا فقـدت قلم الحبر فإنك قد تواجه صعوبة في أخذ الملاحظات في هذا الفصل، لكنك قد تجد قلم رصاص في حقيبتك وسيؤدي الغرض بدون أي مشكلات.

وهنـا مثال آخر: تخيل أن لديـك قائمة تتكون من ١٠ نقاط مـن الأعمال المنزلية وأن عليـك القيام بها في جميع أنحاء المنزل. وأحد هذه الأعمال هو تنظيف غرفتك بالمكنسـة الكهربائية. ومن أجل القيام بذلك عليك اسـتخدام المكنسـة الكهربائية لكن اختك تنظف غرفتها حالياً بالمكنسـة الكهربائية. بالطبع لديك دائماً الخيار في الذهاب والاسـتحواذ على الأصـل إذا كنـت تعتقد أنه مطلوب في هذا الوقت. أو يمكنك أداء بقية المهام أولاً وتأجيل الحاجة إلى هذا الأصل على أمل أن أختك سـتنتهي من اسـتخدام المكنسـة الكهربائية في الوقت الذي ستنتهي فيه أنت من بقية المهام.

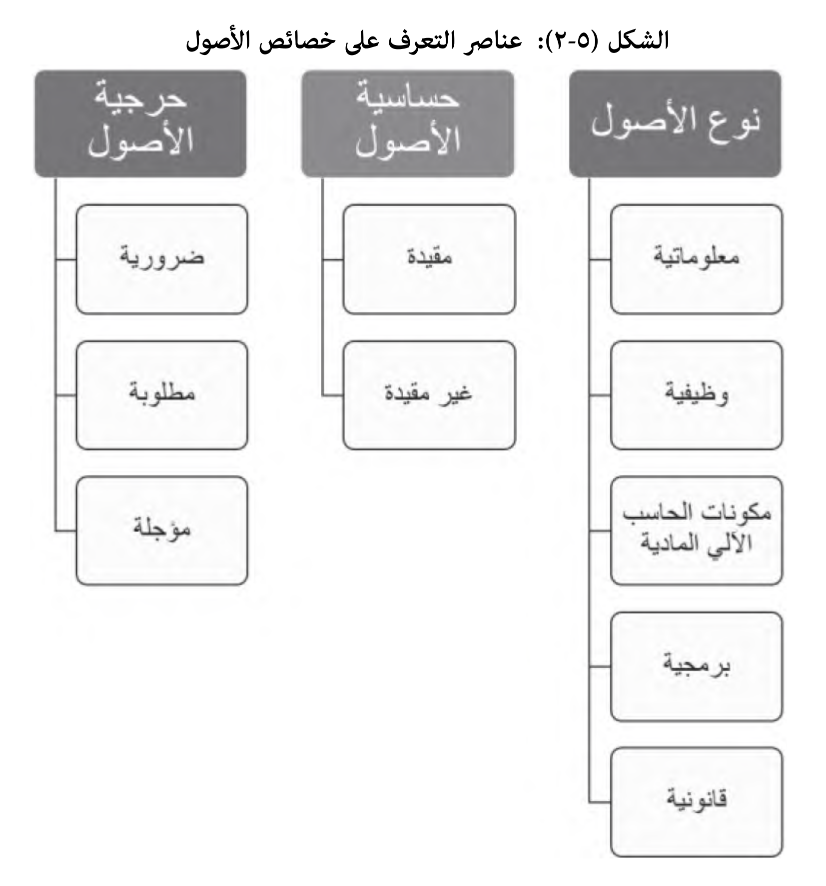
الأصـول المؤجلة هي أيضاً تلك الأصول المعلوماتية التي يمكن إعادة إنشـائها دون تأثير كبير. مثلاً يكتب أستاذك درجاتك الدراسية على ورقة قبل إدخالها في نظام الجامعة الخاص بمعلومات الطلاب. وإذا تعطل جهاز الكمبيوتر الذي يسـتخدمه الأستاذ فجأة وتم فقدان البيانات التي يدخلها فلا تقلق. ما زال لدى الأسـتاذ ورقة الدرجات وبإمكانه إعادة إدخال البيانات المفقودة.

وقد تختلف أيضاً مستويات أهمية الأصول من وقت لآخر. وقد تكون الأصول مرتبطة بها مدى الحياة، قد تكون الأصول حرجة اليوم ما دام مشروع معين على رأس العمل، ولكن بمجرد تسليم المشروع، قد لا تكون هناك حاجة إلى هذه الأصول.

عناصر التعرف على خصائص الأصول موضحة في الشكل (٥-٢).

الجدول (٥-٣) يســتكمل مثال الأصول الســابقة من خلال التعــرف على خصائص تلك الأصول. بعض التعاريف واضحة المعالم، في حين قد تتطلب بعض الخصائص الأخرى شــيئاً مــن التفكــير والنقاش داخل المنظمة. خذ على ســبيل المثال حزمة برامج مايكروســوفت أوفيس (MS Office Suite)، فإن البرامج نفسها بالإضافة إلى «القرص المتعدد الاستخدامات الرقمــي» أو الدي في دي (DVD) الذي يحتــوي على التطبيقات، يمكن اعتبارها أصولاً غير مقيدة لأنك تحتاج إلى المفتاح السري للمنتج حتى تســتطيع تشــغيل التطبيقات. وما دام مفتاح البرنامج مقيداً فإنه يمكن اعتبار حزمة برامج مايكروسوفت أوفيس أصولاً غير مقيدة.

الشكل (٥-٢): عناصر التعرف على خصائص الأصول



الجدول (٥-٣): التعرف على خصائص أمثلة على الأصول من وجهة نظر الجامعة

الأصل	نوع الأصل	حساسية الأصل	أهمية الأصل
جهاز الحاسب الآلي لعضو هيئة التدريس	أصل مكونات الحاسب الآلي المادية	مقيد	مطلوب
الدرجات الدراسية للطالب	أصل معلوماتي	مقيدة	ضروري (مُعتمد على الوقت)
وظيفة محلل أمني	أصل وظيفي	مقيد	مطلوب
حزمة برامج مايكروسوفت أوفيس	أصل برمجي	غير مقيد	مؤجل
ترخيص مايكروسوفت أوفيس	أصل مالي	غير مقيد	مطلوب

وبهذه الجزئية نكون قد أكملنا أساسيات تحديد الأصول والتعرف على خصائصها. لكن مـن الناحية العملية فإن ممارسـة تحديد الأصول وتصنيفها يتطلـب من المُحلل أن يكون على بينة من البيئة التي تعمل فيها الأصول. ويمكن توصيف البيئة من خلال أربعة أبعاد: مرحلة دورة الحياة، وتبعيات النظام، والملكية، والمسؤوليات.

ونمـوذج الحالة المبدئي لهـذه البيئة هو عندما تفكر الإدارة بشراء أصل من أصول تقنية المعلومات من ميزانيتها الخاصة. وفي معظم الحالات فإن المسؤول عن اتخاذ قرار الشراء هو رجـل أعمال يملك خلفية محدودة عن تأثير ذلك النظام على بقية أنظمة تقنية المعلومات. بوصفـك محلل أمن معلومات يملك وعياً عن دورة حياة الأصل، وتبعيات النظام، والملكية، والمسؤوليات، ستكون في وضع أفضل لتوجيه إدخال الأصول في المنظمة. وفي الجزء المتبقي من هذا الفصل سنقوم بتغطية هذه المسائل.

دورة حياة أصول تقنية المعلومات وتحديد الأصول:

تتمتع الأصول بحياة طويلة. وخلال مدة حياتها الصالحة للاستعمال تمر الأصول بمراحل عدة. وفي حين أن معظم مناقشات أمن المعلومات تدور حول الأصول في الاستخدام العملي، نجد أن تحديد الأصول يتطلب التدقيق في جميع مراحل دورة حياة الأصول من أجل تقليل احتمال القضايا الأمنية الناشئة عن استخدام الأصل. ويناقش هذا الجزء دورة حياة الأصول، كـما يطرح أمثلة حول المخاطر المحتملة والناجمة عن الأخطاء غير المقصودة في كل مرحلة من مراحل دورة حياة الأصول.

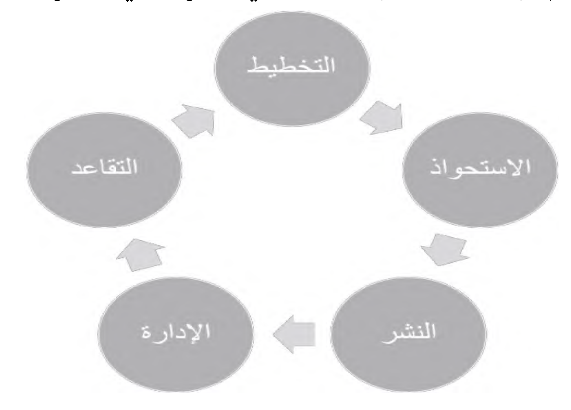
ويوضح الشـكل (٥-٣) الـدورة العامة لحياة أصول تقنيـة المعلومات. وفي مجال أمن المعلومات تسـمى إدارة أصول تقنية المعلومات من خـلال دورة حياتها بإدارة دورة حياة أصول تقنية المعلومات (IT Asset Life Cycle Management).

وتوضـح دورة حياة أصـول تقنية المعلومات الموضحة في الشـكل (٥-٣) المراحل العليا للأصل. وتشمل المراحل التالية: التخطيط، والاستحواذ، والنشر، والإدارة، والتقاعد.

مرحلة التخطيط:

لا تظهر الأصول فقط في نطاق الأعمال بل يتم حيازة الأصول عادة من أجل غرض معين ومـن أجل الإجابة عن ضرورة كمشروع أو كمبادرة. على سـبيل المثال عندما يتم التعاقد مع موظف جديد قد يتخيل الشخص أن أول خطوة ستكون تغييراً في بيئة العمل بشكل أو بآخـر إما بزيادة حمل العمل على الموظفين الحاليين الذين يؤدون مهام معينة، وإما بتلبية الحاجة لمتابعـة الامتثال القانوني والمحافظة عليه وفقاً للقوانين الجديدة، أو الكشـف عن منتج جديد. كما سيتم النظر في تكلفة الأصل في هذه المرحلة.

الجدول (٥-٣): الدورة العامة لحياة أصول تقنية المعلومات



وأحد الأدوات المستخدمة في مرحلة التخطيط هي أداة (طلب المعلومات). وتستخدم هذه الأداة عادة عندما تكون المنظمة غير قادرة على توفير متطلبات ومواصفات محددة للمنتجات، أو غير قادرة على توفير خيارات الشراء. وهذه الأداة من شأنها أن تحدد إلى الموردين بوضوح أن العقد لن يتم اتباعه تلقائياً.

وتُعد مرحلة التخطيط أيضاً أفضل وقت لتقييم عمليات المنظمة في محاولة للاستفادة من الأصل الجديد للمساعدة في مبادرات متعددة. على سبيل المثال، قد يبدأ نشاط التخطيط للحصول على البرمجيات التي من شأنها تشفير البيانات داخل قاعدة البيانات. وقد تكون القوة الدافعة للحصول على الأصول هي ضرورة الامتثال لقوانين الدولة. مثلاً هناك قوانين تتطلب أن تكون أرقام الضمان الاجتماعي مشفرة كلما تم حفظها في نظام معلومات الطالب. لكن وبالتخطيط المناسب فإن ترخيص البرمجيات نفسها يمكن أن يشمل أيضاً أرقام بطاقات الائتمان التي تم حفظها من قبل الكمبيوتر المحلي، كما يمكن أن يشمل نُسَخ من الإقرارات الضريبية التي تم حفظها بواسطة قسم المساعدات المالية.

ولعل أفضل مثال معروف للأخطاء غير المقصودة في مرحلة التخطيط هو عدم وجود ميزات أمنية مصممة في الإنترنت. ففي مراحل التخطيط، لم يتوقع أحد إلى أي مدى هذه التكنولوجيا سوف تُستخدم في المعاملات التجارية في جميع أنحاء العالم حيث كان المخططون مهتمين أساساً بتوصيل البيانات بشكل فعال. وهذا الإغفال مسؤول جزئياً على الأقل عن القضايا الأمنية التي نواجهها اليوم على شبكة الإنترنت.

ومثـال آخر مثير للاهتـمام عن الأخطاء غـير المقصودة في مرحلـة التخطيط هو عدم وجود ميزات أمنية في ويندوز ٩٥ (Windows 95) حيث تم تطوير هذه التقنية لمساعدة المســتخدمين على التواصل عبر الشـبكات الصغيرة في البيئة التي يمكن السيطرة عليها مثل المنازل والمكاتب الصغيرة. وبما أن التركيز كان على راحة المســتخدم، لم يتوقع أحد الاعتماد الواسـع النطاق للإنترنت واستخدام نظام التشغيل (Windows 95) للوصول إلى الإنترنت. وبدون أي حماية أصبحت هذه الحواسيب الإلكترونية أهدافاً سهلة للمهاجمين. وفي الواقع يعتقد بعض خبراء الأمن أن صناعة أمن المعلومات تدين بوجودها للانتشار الواسع لأجهزة ويندوز ٩٥ (Windows 95) غير الآمنة على شبكة إنترنت غير آمنة أيضاً[١٤].

وأخـيراً تأمل من خلال مرحلة التخطيط في متوسـط عمر الأصـل والحاجة المحتملة لبديل في نهاية حياة الأصل. ماذا سيحدث للأصل عندما يصل إلى نهاية حياته في مشروع معين؟ هل ستكون المنظمة قادرة على إعادة استخدامه لمشروع آخر؟ على سبيل المثال، محطة العمل المُستخدمة في تطوير الألعاب الثلاثية الأبعاد والتي تم تخصيصها في البداية لمصممي الألعاب يمكن إعادة تعيينها بعد عام واحد إلى مساعد إداري وذلك لزيادة العمر الإجمالي للأصل في المنظمة.

مرحلة الاستحواذ:

بعد مرحلة التخطيط تأتي مرحلة الاستحواذ. وترتبط المخاوف الرئيسية في هذه المرحلة باســتمرارية بقاء شركة التوريد، كما ترتبط أيضاً بالامتثال للأنظمـة والإجراءات التنظيمية الداخليـة، والجـدوى العمليـة للأصول والمبـادئ الأخلاقية. ويمكـن أن ينطوي ذلك على مجموعة متنوعة من الأسـاليب والتعقيدات المحتملة. ومعظم المنظمات تتطلب سلسـلة من الموافقات للتأكد من أن الأصل الجديد يلبي هذه الشروط. وفيما يلي بعض الإجراءات المستخدمة في هذه المرحلة من دورة حياة الأصول:

دعوة للتفاوض (Invitation to Negotiate): وهي عبارة عن بيان صادر من المنظمة يدل على اسـتعدادها للنظر في المنتج أو الخدمة. ويُعد الإعلان التجاري على سـبيل المثال دعوة للتفاوض حيث المنظمة لديها منتج ومسـتعدة لبيع هذا المنتج بسعر معين. ويجب

(14) Dan Geer, talk at Tampa Bay ISSA chapter annual meeting. 2011

أن نضـــع في الاعتبار أن الـــرد على دعوة التفاوض تختلف عن العـــرض الفعلي ولا يمكن أن يؤدي الرد على الدعوة في حد ذاته إلى التعاقد. وعادة ما تستخدم دعوة التفاوض من قبل الجهات الحكومية عندما تكون معايير الشراء أكثر من معيار السعر المنخفض وحده.

طلـــب تقديم العروض (Request for Proposal): يتم إصدار طلب تقديم العروض عند معرفة أهداف المبادرة أو المشروع، ولكن المنظمة لا تهتم بكيفية تحقيق تلك الأهداف. قد يكون هناك العديد من الطرق التي يمكن اتباعها لإنجاز المهمة، وتقوم المنظمة بالنظر في جميع الخيارات المتاحة. ويحتوي طلب تقديم العروض على تعليمات مفصلة تحدد عناصر المعلومـــات أو الوثائق وذلك لتقديمهـــا لأغراض التقييم. وبالتحديـــد يحتوي طلب تقديم العـــروض عادة على وصف للمنظمة المصدرة لطلب تقديم العروض، وشرح حالي للحالة أو للمـــشروع، أو التحديات التي تواجه المنظمة، وإعـــداد الميزانية والإطار الزمني، ومجموعة أسئلة مفتوحة ليتم الرد عليها من قبل المورد.

دعوة تقديم العطـــاءات (Invitation to Bid): وتُســـتخدم دعوة تقديم العطاءات عندمـــا تكون متطلبات شراء الأصـــول أو الخدمة معروفة ومحددة بشـــكل جيد. وتعتمد دعوة تقديم العطاءات عادة على قيام المُستجيب بتقديم الحد الأدنى من الوثائق التي تدعم بأنه قادر على توفير الســـلع أو الخدمات. وقد تشـــمل أمثلة الوثائق المطلوبة: التراخيص والتصاريح، والتأمين، وإثبات موافقة مصدر المنتج، والمراجع، والمعدات المتاحة، والسنوات، والخبرة في أداء الخدمات المطلوبة. وعند وفاء المستجيب لمتطلبات الحد الأدنى يكون القرار بالتوصية إلى المُستجيب ذي العطاء الأقل.

> يُعد الفشل الموثق لمشروع نظام رواتب مدينة الوقت بمدينة نيويورك (New York City's City Time) مثالاً واضحاً على الاستحواذ غير المناسب. وبغض النظر عن ارتفاع التكاليف، أدى المشروع إلى تحقيق جنائي في مخطط رشوة مزعوم تورط فيها موظفون سابقون في شركة تكامل النظم (SAIC) وشركة التعاقد من الباطن (TechnoDyne). ومقارنة مع الميزانية الأولية والبالغة ٦٣ مليون دولار فإن التكاليف قد بلغت ما يقدر بنحو ٧٦٠ مليون دولار حيث وافقت شركة (SAIC) على دفع (٥٠٠,٤) مليون دولار لتسوية القضية[15].

(15)https://www.washingtonpost.com/business/capitalbusiness/citytime-fallout-continues-for-saic/2012/04/13/gIQA71QtJT_story.html

مرحلة النشر:

مرحلــة النشر هي المرحلة التــي يتم فيها إتاحة الأصول لموظفــي المنظمة. ويتضمن الاهتمام الأساسي في هذه المرحلة: التوافق بين الأصل الجديد مع الأصول التنظيمية الحالية، والتكامل مع الأنظمة الأخرى للمنظمة، وتجنب فقدان البيانات، وتقليل وقت التعطل عن العمــل. ويختلف تعقيد مرحلة نشر الأصول الجديدة اختلافاً كبيراً باختلاف الأصول، وأحد أدوات التفاضــل هو تحديد ما إذا كان الأصل منتجاً جديداً، أو كان نوعاً من البرمجيات، أو كان مبادرة في مقابل تحديث الأصول الموجودة.

أحد أمثلة النشر البسيطة هو نشر جهاز حاسب آلي جديد للموظف. وفي حين أن ذلك يبدو بسيطاً، دعونا نفكر في هذا الوضع قليلاً. لتبسيط الصيانة، لدى معظم المنظمات حداً أدنى من متطلبات الآلات الجديدة ســواء تم نشرها أم لا. وسيكون جهاز الحاسب الآلي الجديد مرخصاً بإصدار معين من نظام التشــغيل، على ســبيل المثال ويندوز ٧ هوم (Windows 7 Home)، لكــن المنظمة لديها ترخيص ودعم نظــام (Windows 7 Professional). لذا وقبل القيام بأي شيء آخر، يجب أن تُمسح بيانات الحاسب الآلي ويجب أن يُعاد تثبيت نظام التشغيل. ومــن ثم نقوم بتثبيت تطبيقات مثــل (Microsoft Office) و(Adobe Acrobat). وإذا كان هناك مجال نشــط (Active Directory) فإن جهاز الحاسب الآلي يجب أن ينضم إلى هذا المجال. كما أن الموارد الأخرى مثل محركات الأقراص والطابعات المشــتركة يتم إتاحتها للجهاز الجديد. وبما أن تركيزنا على أمن المعلومات فإن علينا أن نذكر بأن برنامج مكافحة الفيروســات ســيكون واحداً من أهم الأولويات. وبناءً على ذلك ســيتم التأكد من تثبيت وتحديث برامج مكافحة الفيروسات قبل تسليمها إلى المستخدم النهائي.

ولتقليل وقت التوقف عن العمل بســبب التحديث (تذكّر المبادئ الثلاثة: الخصوصية (Confidentiality)، والتكامــل (Integrity)، والجاهزية (Availability)، تتمثل الخطوة الأخــيرة في نقل ملفات البيانات إلى الجهاز الجديد بمــا في ذلك الصور والعلامات المرجعية. وخــلال هذا الوقت لن يتمكن المســتخدم من العمل على الجهــاز القديم ولا على الجهاز الجديد. وقد يتم تحديد موعد الانتقال من الجهاز القديم إلى الجهاز الجديد بعد ساعات للتقليل من تأثير التغيير، أما إذا كان المستخدم أحد المسؤولين الكبار في المنظمة فعند ذلك لن يتم الشعور بالارتباك في هذه العملية.

هل اكتملت مرحلة النشر؟ لا لم تكتمل بعد حيث لا ينبغي أن تُعد مرحلة النشر كاملة إلا بعد إتاحة الفرصة للمســتخدم النهائي للجلوس واختبــار الجهاز الجديد. وتُعرف هذه الفترة باختبار قبول المســتخدم (User Acceptance Test). ويجب تثبيت التطبيقات غير الموجــودة، كما يجب تأكيد صلاحيات وصول الكتابة والقراءة في الأقراص المشــتركة. وعند ذلك فقط تكون مرحلة الانتشار قد اكتملت.

في عام ٢٠١١ تم نشر نظام جديد لتهيئة الطالب في جامعة جنوب فلوريدا. ولأن النظام كان جديداً ولم يكن بديلاً لتطبيق موجود، لم يكن هناك قلق بخصوص عدم توافر الجاهزية أو حول التوقف عن العمل. وينبغي أن يتم دمج نظام التهيئة الجديد بشكل صحيح مع التطبيق الذي يحفظ بيانات الطالب وهو نظام معلومات الطالب. ويتوجب أن يكون الطالب قادراً على الوصول إلى الواجهة الأمامية الإلكترونية لإدارة بيانات التهيئة، كما يتوجب أن يكون المشرف الأكاديمي قادراً على الدخول إلى النظام لإدخال معلومات الطالب. وكلا العمليتين يتطلب التكامل مع نظام التوثيق المركزي للجامعة.
بدأت مرحلة اختبار قبول المستخدم تجريبياً بـ ١٠٠ طالب مع مشرفيهم الأكاديميين. ومع انتهاء هذه المرحلة والتأكد من أن جميع قضايا التكامل تم حلها، تم توسيع نطاق النظام ليشمل بقية الطلاب وبذلك تم نشر النظام.

وهذا مثال مُبسط على مرحلة النشر. وفي ضوء هذا المثال تأمل في نشر نظام جديد للتحكم الإشرافي والحصــول على البيانــات (Supervisory Control and Data Acquisition) في محطة توليد كهرومائية. ومع أن العملية معقدة وشــاقة للغاية فإن المهام متشــابهة جداً. على ســبيل المثال، إذا كنت تعمل في شركة تبيع هذا النظام فإن المهندسين الذين سيعملون عــلى هذا النظام هم عمــلاؤك. ولأن الهدف هو الحفاظ على الإضاءة في بيوت الناس فإنه يتوجب تركيب النظام الجديد بالحد الأدنى من التأثير في مســتخدمي المرافق الكهربائية في المنــازل. ومن أجل تبســيط الموضوع يمكننا أن نفترض أن المصنــع لديه نظام إضافي يمكن تشــغيله حتى يتم الانتهاء من العمل على النظام الجديد. وأخيراً فإن عملية اختبار النظام في غايــة الأهمية. هل الضوابط تعمل كما تم تصميمها؟ هل تقنيات التعطل الآمن (fail-safe mechanisms) في المكان المناســب لتجنب الأعطــال الخطيرة؟ هل الاختبار العملي، والتفاصيل الرئيسية للنظام ُستُكمَلت بدون عطل؟ هل الاختبارات العملية ناجحة؟

مرحلة الإدارة:

مرحلــة الإدارة هي المرحلة التي تكون فيها الأصول قيد الاســتخدام. فعند الانتهاء من نشر الأصول يجب التأكد من أنها لا تطرح ثغرات جديدة للمنظمة. وبالنســبة للمبتدئين، دعنا نبدأ بمثال صغير يركز على جهاز الحاسب الآلي الذي تم تركيبه مؤخراً.

صافح الموظف وهو في غاية الســعادة موظــف خدمات الدعم الفني الذي قال جملته المعتادة «إذا واجهتك أي مشــكلة اتصل بالدعم الفني وســنأتي لحل المشــكلة على الفور»، وبعد ذلك انتقل الموظف مع جهاز الحاســب الآلي الجديد إلى التحدي التالي. وعلى الرغم مــن أن الدعم الفني وجهاً لوجه قد انتهــى في الوقت الحاضر، فإن هناك الكثير من الأمور التي تحدث في الواجهة الخلفية والتي تُعد في كثير من الأحيان غير مرئية للمستخدم.

وشيء واحد نود أن نفعله هو التأكد من مكان نشر الجهاز، ومعرفة المستخدم الرئيسي للجهــاز، إذا كان ذلــك ممكناً للتطبيق، وكذلك معرفة العنــوان المادي (MAC Address) للجهاز (حتى نتمكن من تتبع الجهاز على الشبكة). وهذا يساعد على تتبع الأصول والذي سنناقشــها لاحقاً في هذا الفصل. وهناك العديد من الطرق للقيام بذلك، بدءاً من جداول البيانات المبســطة للمنظــمات الصغيرة ووصولاً للبرمجيات الآليــة الكبيرة التي يتم نشرها عادة مع الجهاز.

ومن وجهة نظر أمنية، هناك عنصر أساسي يجب القيام به دورياً من أجل الحفاظ على أمــن الجهاز وعلى بيئة آمنة للحوســبة التنظيمية وهو: التحديثــات الأمنية والتصحيحات (patches and security updates). وســنناقش هــذا العنصر بشــكل مطول في الفصول القادمة لكن في الوقت الحالي يكفي القول بأن التصحيحات ضرورية لكل من نظام التشغيل والتطبيقات وبرامج مكافحة الفيروسات.

وعلى الرغم من أنه تم التخطيط مبدئياً ليكون هناك نهاية لحياة أصول تقنية المعلومات، على ســبيل المثال بعد ثلاث ســنوات، إلا أن الحقيقة القاســية للعديد من تلك الأصول هو ارتباطهــا بقيود الميزانية والتي تــؤدي لتمديد حياتها في المنظمة. وفي كثير من الأحيان يتم تطبيــق مبدأ «إذا لم يتعطل لا تقم بإصلاحه» على تلك الأصول ومن ثم فإن المنظمات تجد

نفسـها تديـر أجهزة عفا عليها الزمـن. ومن المهم في هذه الحالة خصوصـاً مواكبة عقود البرمجيـات وصيانة الأجهزة لأطول فترة ممكنة. وسـيأتي الوقت الـذي تكون فيه تكاليف الصيانـة تفوق تكلفـة الجهاز الجديد. وهـذه نقطة واضحة لتنبيـه الإدارة للتوقف عن استخدام الجهاز الحالي القديم ولأن نستبدل به جهازاً جديداً.

مرحلة التقاعد:

مرحلة التقاعد هي المرحلة التي يتم فيها التوقف عن اسـتخدام الأصل الذي لا يشـارك في تحقيـق رسـالة المنظمة. ولا يحدث "التقاعد" دائماً بسـبب شيء عفـا عليه الزمن بل إن السـبب الشـائع لإحالة جهاز ما للتقاعد هو أن إزالته تكون أرخص من الاسـتمرار في استخدامه. والسبب الآخر هو استخدام أصول أحدث وأفضل مع ميزات متطورة.

ويتركـز الاهتمام الرئيـسي في هذه المرحلة على حماية الملكيـة الفكرية للمنظمة وأداء الواجبات الائتمانية. وتحتوي الأجهزة المُراد إحالتها للتقاعد عادة على بيانات، وبعض تلك البيانـات يمكن أن تكـون بيانات مقيدة. ومن المهم التأكد مـن أن هذه البيانات لا يمكن اسـتردادها من الأجهزة المُراد إحالتها للتقاعد. على سـبيل المثال، قد تصل أجهزة الحاسب الآلي المنتـشرة في أحد الكليات إلى مرحلة تكون فيها غـير قادرة على توفير الحد الأدنى من الخدمات للعميد وللطلاب، ويجب أن تحال هذه الأجهزة للتقاعد. وخلال مدة انتشـارها مـن المحتمل أن يكون المسـتخدمون قد سـجلوا عـلى الجهاز بيانات الطـلاب، وبطاقات الائتمان، وغيرها من البيانات الحساسـة. وكجزء من إحالة تلك الأجهزة على التقاعد يجب أن تُمحى جميع تلك البيانات.

وفي الفصـول اللاحقة سـنناقش كيفيـة التخلص من الأجهزة. ويبقـى التبرع دائماً أحد الخيارات، لذا تأكد أنه تم مسح البيانات من الجهاز قبل التبرع به. وإذا كان لدى منظمتك عقـد مع منظمة أخرى للتخلص من المواد، تأكد من وجود بند الخصوصية في العقد وتأكد من وجود تعهد بأن الأجهزة التي تحتوي على البيانات سيجري التخلص منها بشكل مناسب، وليـس فقط القيام بتهيئة الأجهزة لإعادة اسـتخدامها في أغراض أخرى أو إلقاؤها في مكب النفايات.

متى يكون «إحالة الأجهزة للتقاعد» أمراً غير قابل للتغيير؟ افترض أن أستاذاً في كلية الهندسة قد جلب ١٠٠ مليون دولار من أموال المنح إلى الجامعة. بحوث هذا الأستاذ مهمة جداً إلى الكلية. لكن الأدوات التي يستخدمها تتطلب اتصالاً بالشبكة، وتعمل أدوات الأستاذ حالياً على أجهزة قديمة بنظام تشغيل ويندوز ٢٠٠٠ (Windows 2000) إذ لم تعد مايكروسوفت تصدر أي تصحيحات لهذا النظام. هل حان الوقت للإعلان عن أن الجهاز أصبح مستهلكاً ويتوجب إزالته من الشبكة؟

الجواب: الحقيقة هو أنه لا يوجد شيء غير قابل للتغيير. فالقرار الذي يجب اتخاذه في هذه الحالة لا يعتمد على الجانب التقني فقط، بل يجب النظر أيضاً إلى البعد السياسي وعدم الاكتفاء بالمستوى الفني. وتتمثل وظيفة المحلل الأمني الجيد في توفير المعلومات بحيث يتمكن المديرون من اتخاذ قرار مستنير يستند إلى حقائق متوازنة من الجهة التقنية والقانونية والسياسية وحتى التداعيات ذات الصلة بوسائل الإعلام.

فلنأخذ المثال الذي ناقشناه في الفصل الثاني. جامعة ولاية الشمس المشرقة تخطط لاستبدال نظام البريد الإلكتروني الحالي بنظام جديد يعتمد على الحوسبة السحابية ويوفر الاستقرار والبديل الاحتياطي ومميزات جديدة لمجتمع المستخدمين. وفي الوقت نفسه سيسمح ذلك للجامعة بتهيئة أصولها الوظيفية لإعادة استخدامها في أغراض أخرى تدعم رسالة الجامعة. وفي وقت لاحق سنناقش التأثير المُحتمل للاستخدام المستمر لجهاز انتهت حياته الافتراضية في الجامعة وكما سنقوم بتحليل مخاطر ومنافع هذا الدعم.

ونذكر هنا مثالاً لما يمكن أن يحدث نتيجة لضعف إجراءات مرحلة التقاعد. ففي عام ٢٠٠٩ تم شراء قرص صلب من موقع إي باي (eBay) ووُجد أن هذا القرص يحتوي على تفاصيل الدفاع الصاروخي الأمريكي حيث يعود هذا القرص لشركة لوكهيد مارتن (Lockheed Martin)، وهي شركة متعهدة في وزارة الدفاع الأمريكية.

التحديد النمطي لمواصفات النظام (System Profiling):

في الأمثلة السابقة نظرنا إلى الأصول منفصلة عن بعضها: جهاز حاسب آلي محمول، وخادم، ومجموعة بيانات محددة. وقد تم ذلك بهدف التبسيط خلال مقدمة الموضوع.

لكن عند تقييم الأهمية والحساسية في الواقع العملي فإنه من الضروري النظر إلى الأصول في سياق النُظم التي تُستخدم فيها.

الأصل الذي قد يعد «ضرورياً» وهو منفصل، وقد يتم تصنفيه بأنه أصل «مطلوب» في الواقع العملي إذا كانت المنظمة استثمرت بشكل كاف في البديل الاحتياطي. وبالمثل فإن الأصل الذي يمكن أن يعد «مؤجلاً» وهو منفصل يمكنً في الواقع أن يكون أصلاً «ضرورياً» عند النظر إليه في سياق النظام (ترخيص نظام الجدولة في شركة الطيران على سبيل المثال). ويمكن أن تُعد مجموعة من الأصول الفردية في حد ذاتها أصولاً «مؤجلة» لكن بالنظر إليها بوصفها مجموعة يمكن أن تُعد أصولاً «حرجة». ويقدم هذا القسم عرضاً موجزاً للتحديد النمطي لمواصفات النظام.

ويُعد التحديد النمطي لمواصفات النظام أكثر تعقيداً من قائمة جرد مبسطة لأجهزة الحاسب الآلي. إن تحديد جميع مكونات النظام والاعتمادية بين تلك المكونات قد يكون فناً بقدر ما هو علم. التحديد النمطي لمواصفات النظام هو تجميع كل الأصول التي تم جردها، وتصنيفها حسب الوظيفة، وفهم الاعتمادية بين تلك الأصول. بمعنى آخر هو تكوين رؤية مكبرة لنظام أو عملية معينة.

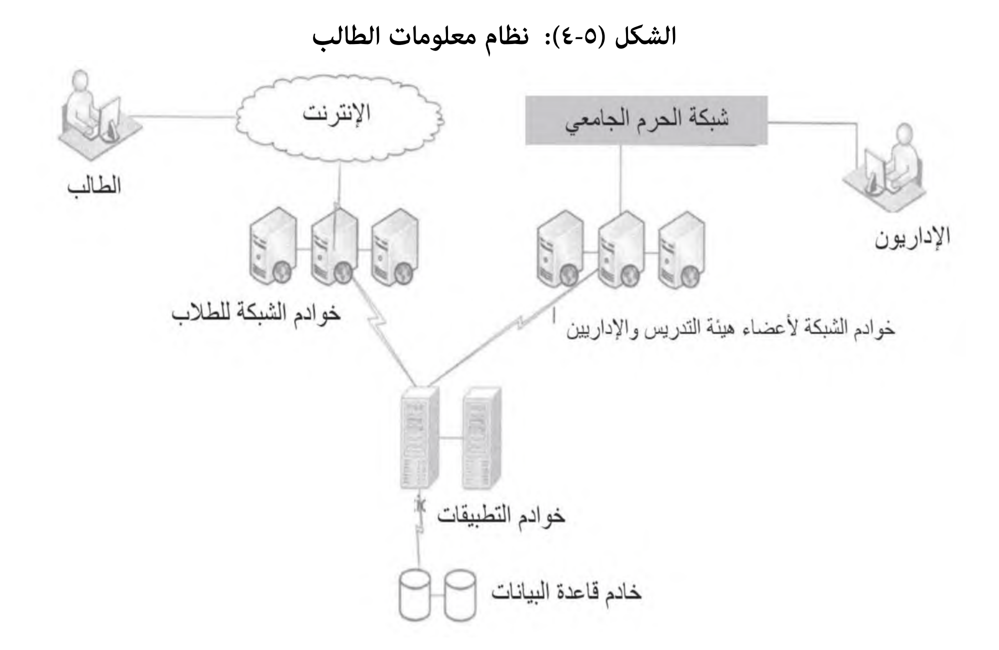
ووفقاً لتوجيهات إدارة مخاطر تقنية المعلومات (NIST SP800-30) الصادرة عن المعهد الوطني للتقنية والمعايير (National Institute of Standards and Technology)[١٦]، فإن المنظمة تعمل على توفير الأجهزة والبرامج وواجهات النظام، والبيانات، والموظفين، ومهام النظام وذلك أثناء أداء التحديد النمطي لمواصفات النظام. ونتيجة لذلك سيتم تحديد حدود النظام بشكل واضح جنباً إلى جنب مع الوظيفة والأهمية والحساسية.

تأمل مرة أخرى في البيئة الجامعية، وبالتحديد تأمل في بعض أنظمة تقنية المعلومات الموجودة في الجامعة لتشغيل الجانب الأكاديمي والجانب المهني من بيئة التعليم. إن نظام معلومات الطالب (Student Information System) الموضح في الشكل (٥-٤) هو أحد تلك الأنظمة الأساسية.

---

(16)NIST SP800-30 ،http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

الشكل (٥-٤): نظام معلومات الطالب



نظام معلومات الطالب:

يقوم نظام معلومات الطالب بالوظيفة التي يدل عليها اسم هذا النظام: يقوم النظام بتخزين معلومات الطالب مثل المساعدات المالية، والدرجات، والعنوان، ورقم الضمان الاجتماعي، وبيانات الإرشاد الأكاديمي، وجدول المحاضرات. وهذا النظام جزء حيوي من عمليات الجامعة. ويوضح الشكل (٥-٤) عينة من نظام معلومات الطالب. ويستطيع الطلاب استعراض معلوماتهم من خلال واجهة مستعرض الإنترنت. ويستطيع كل من المشرفين الأكاديميين والأساتذة والمسؤولين الآخرين من استعراض المعلومات بنظرة أعمق من خلال واجهة جهاز الحاسب الآلي المكتبي.

ووفقاً لتوجيهات إدارة مخاطر تقنية المعلومات (NIST SP800-30)، يمكننا التعرف على مواصفات النظام على النحو التالي.

مكونات الحاسب الآلي المادية:

تتكفل البدائل الاحتياطية لخوادم الشبكة الخاصة بالطلاب بالتعامل مع واجهة الطلاب. وكل خـادم في حـد ذاتـه يُعد أصلاً مؤجلاً: بالإمـكان أن يتعطل أحدها لكـن كل ما يراه المستخدم النهائي هو تأثير بسيط جداً في الأداء يتثمل في تأخير بسيط في تحميل الصفحات. لكن الخوادم مجتمعة تمثل أصولاً مطلوبة: إذا تم بطريقة ما فقدان اتصالها بالإنترنت فإن الطـلاب لن يكونـوا قادرين للوصول إلى تلك الخوادم. وتصبـح تلك الخوادم خلال فترات التسجيل أصولاً ضرورية: إذا فقدت اتصالها بالشبكة فلن يكون أحد قادراً على التسجيل.

ويمكن إجراء تحليـل مماثل على جميع عناصر النظام، كما يمكن فصلها إلى نظم فرعية بمستويات مختلفة من الأهمية والحساسية.

البرمجيات:

يُعـد نظام معلومـات الطالب من الأنظمة المعقدة جداً التـي لا يمكن تطويرها داخل الجامعـة. وهناك أنظمة تجارية وأنظمة المصـادر المفتوحة لنظام معلومات الطالب مثل (Ellucian›s Banner) و(OpenSIS). ويحتوي التطبيق على العديد من المكونات المعقدة وغالبـاً ما تتضمن الواجهة الخلفية قاعدة بيانات حيث يتم تخزين جميع المعلومات فيها. وتكـون واجهة الطالب معتمدة على واجهة الشـبكة، أما واجهة أعضـاء هيئة التدريس/ الموظفـين فتكون واجهة مخصصة. ويُنظر عـادة إلى جميع البرمجيات والتراخيص المرتبطة بأنها أصول ضرورية.

البيانات:

مـا نوع البيانات التي سـيجري حفظهـا في نظام معلومات الطالـب؟ يبرز هنا نوعان مـن البيانات والتي يجب التعامل معهـما بأنها من البينات المُقيدة: الدرجات الدراسـية وأرقام الضمان الاجتماعي. الدرجات الدراسـية هي معلومات لا يسـمح بنشرها في دليل الطالـب وهي محمية بقانون الحقوق التعليمية والخصوصية للأسرة لعام ١٩٧٤ (Family Educational Rights and Privacy Act) كما رأينا سابقاً في هذا الفصل. وأرقام الضمان

الاجتماعي (وبقية معلومات التعريف الشــخصية) أيضاً محمية بقانون الحقوق التعليمية والخصوصية لــلأسرة بالإضافة إلى أنظمة الولاية والأنظمة الفيدرالية الأخرى. وإجمالاً فإنه وبســبب نوع البيانات التي تحتوي عليها أنظمة معلومات الطالب فإن هذه النظم تصنف بأنها نظم مُقيدة.

واجهات النظام:

واجهــات النظام تحدد كيفية إدخال البيانات وكيفية اســتخراجها من النظام. تأمل في المدخلات التالية:

- القبول: كيف يتم قبول الطالب في الجامعة؟
- المتقدمون: هل هناك واجهة منفصلة يستخدمها المتقدمون لبرامج الجامعة؟
- المساعدات المالية: هل هناك أي متطلبات للإبلاغ عن المساعدات المالية؟ ماذا عن الاعتبارات الضريبية؟
- المنح الدراسية: كيف يتم مَنح المِنح الدراسية والإبلاغ عنها؟
- الامتثال: هل هناك أي متطلبات للإبلاغ عن عدد الطلاب، ومتوسط المعدل التراكمي، أو أي نوع آخر من المعلومات إلى إدارة التعليم؟
- الدرجات الدراســية: كيف يتم إدخال الدرجات الدراســية؟ يدوياً أم آلياً من نظام إدارة التعليم؟
- الفصول: كيف يتم إرســال الحذف والإضافة إلى نظام إدارة التعليم بحيث يتضمن النظام معلومات حديثة عن الذين تم تسجيلهم وعن المخولين بالوصول إلى الفصول المعينة؟

كل مــن هذه الواجهات تحتوي عــلى بيانات يتم تبادلها بين نظــام معلومات الطالب وأنظمة أخرى. وإذا كانت تلك البيانات تُعد بيانات مقيدة فإن هذا التبادل يجب تشفيره، أو على الأقل تشفير تلك البيانات المقيدة.

يجب أن تكون بيانات اعتماد المُســتخدم، والتي تُســتخدم للوصول إلى النظام، محمية خصوصاً بيانات اعتماد الحسابات ذات الصلاحيات الواسعة.

من الممكن أن يتضمن التحديد النمطي لمواصفات النظام معرفة التطورات الأخيرة بالأدوات البرمجية. على سبيل المثال، في شهر أكتوبر من عام ٢٠١٠ قام إيريك بتلر (Eric Butler)، وهو مطور لبرمجيات وتطبيقات الشبكة، بإطلاق ملحق لبرنامج فايرفوكس (Firefox) يُدعى (Firesheep) وظيفته الأساسية «الاستماع» لحركة مرور الشبكة على وسائل الإعلام المشتركة، مثل نقاط الدخول إلى شبكة الإنترنت العامة، بحثاً عن البيانات غير المشفرة. والنص التالي من الموقع الإلكتروني لإيريك بتلر[١٧]:

من الشائع كثيراً أن تقوم المواقع الإلكترونية بحماية كلمة السر الخاصة بك عن طريق تشفير الدخول الأولي، لكن من الغريب أن يكون تشفير أي شيء آخر أمراً نادراً. وهذا يترك ملفات الارتباط (cookie) ومن ثم المستخدم عرضة للهجوم. إن اختطاف جلسة بروتوكول انتقال النص المتشعب (HTTP) (والذي يسمى أيضاً sidejacking) عبارة عن اكتساب المهاجم للسيطرة على ملفات الارتباط لمستخدم ما والذي يتيح للمهاجم القيام بأي شيء يمكن للمستخدم القيام به على موقع معين. إن ملفات الارتباط (cookies) في الشبكة اللاسلكية المفتوحة تكون منتشرة في الهواء مما يجعل هذه الهجمات سهلة للغاية.

أداة إيريك هذه ليست جديدة بل هي شكل من أشكال برامج التلصص على الشبكات أو ما يعرف بـ (sniffer). وأحد المواقع الخدمية المعرضة للهجوم من قبل أداة إيريك هو موقع فيسبوك.

وبهـذه الطريقة فإن الهدف من التحديد النمطـي لمواصفات النظام هو وصف النظام مع جميع تبعياته حتى نتمكن من اتخاذ قرار بشـأن ما ينبغي تعديله (وصول المسـتخدم للنظام من خلال وسائل غير آمنة على سبيل المثال)، وتحديد نقاط العطل المفردة (single points of failure) وغيرها من الأمور.

وهناك نظام تقني آخر مهم، بالخصوص في الجامعات ذات التركيز البحثي، وهو نظام الحوسبة العالي الأداء (high-performance computing system). ويتكون هذا النظام عادة من مجموعة من الخوادم تعمل جنباً إلى جنب وتتقاسم فيما بينها المعالج وموارد الذاكرة للعمل على مشكلة واحدة. وليس من النادر أن نرى مئات من الخوادم التي تم تكوينها بهذه الطريقة. وفي هذا الإعداد كل خادم على حدة مصمم أن يكون أصلاً مؤجلاً. وعندما يتعطل أحد هذه الخوادم يكون هناك خلل بسيط جداً في الأداء بحيث يستمر العمل الأساسي. وتم تصميم النظام الشامل ليسمح بنسبة معينة من تلك الخوادم أن تكون خارج الخدمة ومع ذلك يستمر النظام في العمل.

(17)http://codebutler.com/firesheep/

ملكية الأصول والمسؤوليات التشغيلية:

ناقشــنا في بداية هذا الفصل أن الهدف من تحديد الأصول والتعرف على خصائصها هو الجمع الاستباقي لكل المعلومات الضرورية عن أصول المنظمة والتي يمكن أن تكون مفيدة في الاســتجابة للتهديدات التي تؤثر في تلك الأصول. وحتى الآن قمنا بجمع كل المعلومات الفنيــة اللازمة لهــذا الغرض: ما هي الأصــول؟ (تحديد الأصول)، وما مــدى أهمية هذه الأصــول؟ (التعــرف على خصائص الأصــول). ولكن لم نتعرض إلى عنــصر مهم من عناصر الاستجابة للتهديدات التي تواجه الأصول: من الذي يجب أن يرد على تهديد محدد يواجه الأصول؟

ولهذا السبب، وكجزء من التعرف على خصائص الأصول، فإنه من الضروري أيضاً تحديد المسؤولية الفردية عن الأصل. في الشبكة المنزلية الخاصة بك هذا أمر سهل - أنت مسؤول عــن جميع التوصيلات داخــل المنزل، ومزود خدمة الإنترنت مســؤول عن أي شيء يحدث بالاتصــال مع الشــبكة. لكن في شــبكات المنظمات، هــذا الموضوع أكثر تعقيــداً. هناك مشكلتان محددتان من المُحتمل أن تواجههما. المشكلة الأولى هي أنه من المرجح أن يكون أفراد مختلفون أو وحدات مختلفة مسؤولين عن وظائف مختلفة تتعلق بالأصل. والمشكلة الثانيــة هي أنه ليس من المرجح أن تكون قــادراً على توقع كل ما يمكن أن يتعرض له أحد الأصول وذلك على الرغم من محاولاتك الحثيثة لتحقيق ذلك.

المســؤوليات التشــغيلية هي مســؤولية الفــرد أو الوحدة عن وظيفــة محددة تتعلق باستخدام أحد الأصول. وتحدد المسؤوليات التشغيلية دور أعضاء المنظمة المرتبطة بجميع الوظائــف المحــددة مســبقاً والمتعلقة بالأصل. أمــا مالك الأصل فهو فــرد أو وحده يملك مسؤولية تشغيلية لجميع الوظائف غير المتوقعة والمرتبطة بتأمين الأصل.

وقد تلاحظ أن التعريف السابق لمالك الأصل لا يشير إلى الجهة التي تدفع الأموال لشراء الأصول، هذا لأنه كما يمكن تشارك الإسهامات المتعلقة بالميزانية وملكية الأصل، يمكنها أيضاً أن تكون منفصلة بعضها عن بعض. ويمكن توضيح ذلك من خلال المثال التالي.

مخاطر غير متوقعة - قصة حقيقية

في عام ٢٠٠٤ طلب أحد أعضاء هيئة التدريس في جامعة بحثية من رئيس القسم شراء عدد قليل من أجهزة الحاسب الآلي لإعداد مختبر في القسم. وتم وضع أجهزة الحاسب الآلي في غرفة في القسم، وقام عضو هيئة التدريس مع بعض طلاب الدراسات العليا، بتمويل من إدارة القسم، بضبط أجهزة المختبر والبرمجيات التابعة لها.

وهكذا فإن الإدارة الأكاديمية تحملت كافة النفقات المتصلة بالأصول. ولم يكن لوحدة تقنية المعلومات في الجامعة أي دور في إنشاء المختبر، وفي الواقع، لم تكن وحدة تقنية المعلومات مشاركة في العملية.

ولكن في ذلك الصيف تعرض أحد أجهزة الحاسب الآلي في المختبر للاختراق وتم استخدامه بوصفه جزءاً من الروبوتات لتشغيل هجمات القاموس (تخمين كلمات السر) على أجهزة حاسب آلي لوكالة مصنفة بأنها وكالة حكومية اتحادية. وأصبح جهاز الحاسب الآلي في المختبر جزءاً من تحقيقات مكتب التحقيقات الفيدرالي (FBI) وتلقت الجامعة استدعاء رسمي من مكتب التحقيقات الفيدرالي لإنتاج صورة القرص لجهاز الحاسب الآلي. وأحال المستشار العام للجامعة الاستدعاء إلى وحدة تقنية المعلومات في الجامعة. ولأنه لم يكن لدى الإدارة الأكاديمية الخبرة أو الموارد لتقديم صورة القرص، قامت وحدة تقنية المعلومات في الجامعة بإنجاز المهام المطلوبة وقدمت المعلومات اللازمة لمكتب التحقيقات الفيدرالي.

ويجــب أن يكــون واضحاً من المثال أنه بينما دفعــت الإدارة الاكاديمية الأموال لشراء الأصول، فإن المسؤولية التشــغيلية تقع على عضو هيئة التدريس وذلك لجميع الجوانب المتوقعة للأصل بما في ذلك تثبيت البرامج وتحديثاتها، والنسخ الاحتياطي للبيانات، وإدارة حســاب المستخدم. كما ينبغي أن يكون واضحاً من المثال أن استدعاء مكتب التحقيقات الفدرالي كان ســيناريو غير متوقع بأبداً، والذي تم التعامل معه في نهاية المطاف من قبل وحــدة تقنية المعلومات في جامعة جنوب فلوريدا. وفي هذا المثال كان أول تدخل عملي لوحــدة تقنية المعلومــات في المختبر عند تلقي الاســتدعاء. من الــذي يُفترض أن يكون مالــكاً للأصول: الإدارة الأكاديميــة، أو عضو هيئة التدريس، أو وحدة تقنية المعلومات في الجامعة؟

ولأن عمليــات أصول تقنية المعلومات تتطلب مهــارات متخصصة فإن منظمات تقنية المعلومات تكون غالباً مسؤولة عن جميع المهام المتبقية والمتعلقة بأصول تقنية المعلومات. ولأن معظــم أصول تقنية المعلومات يتم شراؤها من قبل وحــدات الأعمال ومن ميزانيتها الخاصــة فإن وحدة تقنيــة المعلومات غالباً لا تُعد مالكة لتلــك الأصول. ويجب أن يكون محلــل النظم على بينة من هذه الديناميكية وعواقبها لأن مالك الأصول هو المســؤول عن تنســيق الجهود لضمان أمان الأصــول. ويمكن أن يكون الفهم الواضــح لهذا الجانب من معرفة خصائص الأصول مفيداً في تخطيط ردود الفعل للمخاطر المحتملة على الأصول.

وفي مثال آخر دعنا ننظر في نوع معين من الأصول المعلوماتية الشــائعة لدى الجامعات وهي «البيانات المؤسســية». وتُعرّف جامعة جنوب فلوريدا البيانات المؤسسية على النحو التالي: تُعرف البيانات المؤسســية بأنها جميع عناصر البيانات التي تم إنشــاؤها والمحافظة عليها واســتلامها أو إرســالها نتيجة لأنشطة الأعمال، أو التعليم، أو البحوث في نظام جامعة جنوب فلوريدا ويمكن أن تشمل واحدة أو أكثر من الخصائص التالية:

- ذات صلة بالعمليــات والتخطيط، والتحكم، ومراجعــة وظائف الأعمال في كل من الوحدات الإدارية والأكاديمية.
- بشــكل عامٍ هي بيانــات مرجعية أو مطلوبة بين أكثر من وحــدة إدارية وأكاديمية. وتكون أيضاً مشمولة في التقرير الرسمي المنشور عن نظام الجامعة.
- يتم إنتاج أو اشتقاق البيانات بواسطة وحدة تابعة لنظام جامعة جنوب فلوريدا أو موظف، أو إحدى الجهات التابعة أو وكيل لنظام جامعة جنوب فلوريدا.
- مصنفة ومقيدة وفقاً لنظام وسياسة جامعة جنوب فلوريدا وقانون الولاية والقانون الفيدرالي.

ومن الســهل أن نرى أنه يمكن توزيع هذا النوع مــن البيانات في جميع أنحاء الجامعة وإلى مجموعة متنوعة من الملاك. ومن المهم توضيح خطوط مســؤولية المستخدمين الذين يتعاملون مع هذا النوع من البيانات. وهنا يأتي دور ملكية الأصول المعلوماتية والمسؤوليات التشغيلية للأصول المعلوماتية.

وبينــما تتوقف الملكيــة الحقيقية للأصول على الجامعة، يجب أن يكون هناك شــخص قادراً على اتخاذ قرار بشــأن اســتخدام البيانات. ومادام الأمــر كذلك فإن الجامعة تفوض الســلطة المتعلقة بأمن البينات المؤسســية ومســؤوليتها النهائية إلى أفراد محددين داخل المنظمة. ويُعرف هؤلاء الأفراد بملاك الأصول المعلوماتية.

أما المســتخدمون الذين لديهم مســؤوليات تشــغيلية للحفاظ على أمن البيانات ولكن لا يملكــون تلك البيانات يُســمون بأمناء البيانات. ويُعــد المشرف الأكاديمي مثالاً على أمين البيانات لأنه يســتطيع الوصول إلى كشــف درجات الطالب بهدف مســاعدته في تســجيل المواد الدراسية الأكثر ملاءمة من أجل التخرج في الوقت المحدد. ويتمتع المشرف الأكاديمي بالمسؤولية الائتمانية للحفاظ على سرية هذه البيانات ولكنه لا يعد مالكاً للبيانات.

العقود غير المكتملة، والملكية، والمسؤوليات المتبقية:

هناك أســاس نظري لتخصيص ملكية الأصول إلى الجهة المسؤولة عن التعامل مع جميع القضايــا غير المتوقعة التي تواجه أحد الأصول. وهذا الأســاس النظري هو «نظرية العقود غير المكتملة». وعموماً يمكن للمشــاركين في معاملة ما عــدم كتابة العقد الذي يتوقع كل الاحتمالات والردود المناسبة لكل احتمال. ومن ثم فإن العقود غير مكتملة بالضرورة، ومن المفيد وضع آلية للتعامل مع القضايا غير المتوقعة عند حدوثها.

الاقتصاديان سانفورد غروسمان (Sanford Grossman) وأوليفر هارت (Oliver Hart) وضعا فكرة «حقوق الضبط المتبقية» (residual rights of control) كآلية ممكنة للتعامل مع هذه الفجوات. و «حق الضبط المتبقي» هو الحق في استخدام الأصل كما تريد باستثناء حقوق الاستخدام التي اُستبعدت صراحةً في العقد. ويقترح الاقتصاديان أن الملكية مرادفة في معناها إلى «حقوق الضبط المتبقية». ويُشــير اســتخدام نظرية العقود غير المكتملة إلى أن الملكيــة (أو الحقوق المتبقية) يجب أن تُســند إلى المجموعــة التي يؤثر مجهودها تأثيراً كبيراً في إنتاجية الأصل، وذلك لأن الحقوق المتبقية تحفز بقية الأطراف وبقوة للاســتثمار في تطوير إنتاجية الأصل.

ماذا عن المســؤوليات الأمنية؟ تُشــير نظرية العقود غير المكتملة إلى أن الجهة المسؤولة التي يجب أن تســند إليها أيضاً ملكية الأصول هي الجهة المســؤولة عن جعل الاستثمارات المتبقية واللازمة للحفاظ على الأصول مفيدة بالنســبة للمنظمة. وهذا سيحفز الجهة على القيام بالاستثمارات المناسبة في الأصول متضمناً ذلك استثمارات أمن المعلومات.

ويمكــن النظر إلى تنظيم تقنيــة المعلومات بوصفه مزوداً لجميــع خدمات دعم تقنية المعلومات في المنظمة. وعلى هذا النحو فإن تحديد ملكية الأصول يتطلب مشــاركة وحدة تقنية المعلومات في مراحل التخطيط لكافة المشــاريع التي تتطلب الدعم التشغيلي لتقنية المعلومات. وهذه المشــاركة تــؤدي إلى وثيقة تدعى باتفاقية مســتوى الخدمة (Service Level Agreement). وهذه الوثيقة تحدد ما تقوم به وحدة تقنية المعلومات وكيف تقوم بذلك وذلك لإنجاز وإدارة توقعات العميل أو مالك النظام.

المراجع:

Grossman, S.l. and Hart, O.D. "The costs and benefits of ownership: a theory of vertical and lateral integration," The Journal of Political Economy, 1986.94(4): 691719-.

Hart, O.D. "Incomplete contracts and the theory of the firm," Journal of Law, Economics and Organization, 1988,4(1): 119139-.

وبهذه الخلفية نســتطيع تحديث جدول التعرف على خصائص الأصول ليشــمل الملكية والمسؤولية على النحو المبين في الجدول (٥-٤).

الجدول (٥-٤): التعرف على خصائص الأصول والملكية والمسؤوليات

الأصل	نوع الأصل	حساسية الأصل	أهمية الأصل	المالك	المسؤوليات
جهاز الحاسب الآلي لعضو هيئة التدريس	أصل مكونات الحاسب الآلي المادية	مقيد	مطلوب	عضو هيئة التدريس	النشر- وحدة تقنية المعلومات، النسخ الاحتياطي - وحدة تقنية المعلومات، التصحيحات - عضو هيئة التدريس
الدرجات الدراسية للطالب	أصل معلوماتي	مقيدة	ضروري	مكتب مراقب مسجل المساعدات المالية	وحدة تقنية المعلومات
وظيفة محلل أمني	أصل وظيفي	مقيد	مطلوب	وحدة تقنية المعلومات	وحدة تقنية المعلومات
حزمة برامج مايكروسوفت أوفيس	أصل برمجي	غير مقيد	مؤجل	المستخدم النهائي	وحدة تقنية المعلومات
ترخيص مايكروسوفت أوفيس	أصل مالي	غير مقيد	مطلوب	وحدة تقنية المعلومات	وحدة تقنية المعلومات

نموذج حالة-ستكسنت (Stuxnet):

تُعد منشأة تخصيب اليورانيوم في مدينة (نطنز) أحد الأصول الإيرانية الأكثر أهمية وحساسية. ويعمل قرابة ٥٠٠٠ جهاز طرد مركزي لتخصيب اليورانيوم بهدف صنع أسلحة نووية، وذلك لكي تتمكن إيران من تطوير قنبلة نووية بنفسها. وإلى جانب ذلك هناك أجهزة حاسب آلي تُستخدم لرصد ومراقبة أجهزة الطرد المركزي.

وتشـعر العديـد من الدول، بمـا في ذلك الولايات المتحـدة، بالقلـق إزاء برنامج إيران النووي. وبعد النظر في جميع الخيارات المتاحة حددت هذه الدول أجهزة الحاسـب الآلي المسـتخدمة في رصد ومراقبة أجهزة الطرد المركزي بأنها أفضل الأصول للاستفادة من إبطاء التقدم الإيراني. وكانت النتيجة دودة حاسـوبية متطورة والمعروفة على نطاق واسـع باسم «ستكسـنت» (Stuxnet). وتفيد التقارير بأن هذه الدودة في ذروة فعاليتها قد استطاعت تعطيل ١٠٠٠ إلى ٥٠٠٠ جهاز مركزي تعمل في مدينة (نطنز) مما أخّر تقدم إيران بنحو ١٨ شهراً.

وقـد تـم تصميم هذه الدودة لتنتشر من جهاز مسـتهدف إلى جهاز آخر تلقائياً لتقوم بأداء وظيفتها ثم تدمر نفسـها دون أن تترك أي أثر وراءها. لكن الأجهزة المستهدفة كانت تخضع لحراسـة مشـددة. ولتحقيق حماية إضافية لم تكن تلك الأجهزة متصلة بالإنترنت، بمعنى أنه لا يمكن لأي هجوم من شبكة الإنترنت الوصول إلى تلك المرافق. ومن وجهة نظر المهاجمين فإن الأشـخاص الذين يعملون في المنشأة يمثلون أصولاً مفيدة جداً. فإذا كان من الممكن إقناع شـخص واحد بحمل قرص يو إس بي (USB thumb drive) مصاب بالدودة إلى المنشـأة فإنه يمكن للدودة البدء بالقيام بعملها. وبناء على ذلك يمكننا افتراض أن هذا ما حدث بالضبط.

وتُعد ستكسنت الدودة الحاسوبية الأولى في العالم التي استخدمت كسلاح.

المراجع:

Sanger, D.E. "Obama order sped up wave of cyberattacks against Iran," New York Times, June 1,2012.

Ed Barnes, "Mystery surrounds cyber missile that crippled Iran's nuclear weapons ambitions," Fox News, November 26, 2010, http://www.foxnews.com/tech/201026/11//secret-agent-crippled-irans-nuclear-ambitions.html (accessed 2/4/2013).

الملخص:

ناقشنا في هذا الفصل موضوع تحديد أصول تقنية المعلومات والتعرف على خصائصها في المنظمة. ويمكن أن تكون الأصول أصولاً عامة أو أصولاً ذاتية، كما أن تحديد الأصول يتطلب اهتماماً وثيقاً بالاحتياجات الفريدة للمنظمة والموارد التكنولوجية الضرورية لنجاح المنظمة في تحقيق رسالتها. ويجب التعرف على خصائص الأصول التي تم تحديدها من أجل جمع كافة المعلومات الضرورية لحماية الأصول في أوقات الحرب والسلم. ويشمل التعرف على خصائص الأصول تصنيفها بناءً على الحساسية وأهمية الأصول. كما يجب تعيين المسؤوليات الفردية لجميع المسائل المعروفة وغير المعروفة والمتعلقة بأمن المعلومات والتي قد تنشأ أثناء استخدام الأصل.

أسئلة مراجعة للفصل:

١. ما الأصول من وجهة نظر أخصائي أمن المعلومات؟

٢. خلال عملية تحديد الأصول، لماذا من المهم البدء بتحديد الأصول المهمة بالنسبة للمنظمة؟

٣. ما الطريقتان الأكثر شيوعاً لمعرفة ما هو مهم بالنسبة للمنظمة؟

٤. ما الأصول العامة؟ ما الأصول الذاتية؟ ما الفرق بينهما من جهة الجهد اللازم لتحديد كل منهما بالشكل الصحيح؟

٥. ما قائمة المراجعة؟ ولماذا تُعد قوائم المراجعة مفيدة في قطاع الأعمال بشكل عام؟[١٨] ولماذا لا تُعد قوائم المراجعة مفيدة جداً في تحديد الأصول؟

٦. ما الغرض من بيان رسالة المنظمة (Mission Statement)؟ ما الغرض من بيان رؤية المنظمة (Vision Statement)؟ وما هو الفرق بينهما؟

٧. ما الأصل المعلوماتي؟ أعط بعض الأمثلة.

---

(١٨) لمزيد حول هذا الموضوع، ننصح بشدة الاطلاع على هذا الموقع الإلكتروني والكتاب الموجود على الرابط: http://atulgawande.com/book/the-checklist-manifesto/

٨. ما الأصل الوظيفي؟ أعط بعض الأمثلة.

٩. ما أصل مكونات الحاسب الآلي المادية؟ أعط بعض الأمثلة.

١٠. ما الأصل البرمجي؟ أعط بعض الأمثلة.

١١. ما الأصل القانوني؟ أعط بعض الأمثلة.

١٢. اذكر بعضاً من العناصر المهمة للمعلومات الخاصة بأصول مكونات الحاسب الآلي المادية والتي يجب تتبعها. وما الهدف من ذلك التتبع؟

١٣. ما عملية التعرف على خصائص الأصول؟ ولماذا تُعد مفيدة؟

١٤. ما حساسية الأصول؟ وما فئات الحساسية الشائعة التي تستخدم في التعرف على خصائص الأصول؟

١٥. ما أهمية الأصول؟ وما فئات الأهمية الشائعة التي تستخدم في التعرف على خصائص الأصول؟

١٦. ما دورة حياة أصول تقنية المعلومات؟ وما مراحل دورة الحياة تلك؟

١٧. ما اهتمامات أمن المعلومات خلال مرحلة التخطيط من دورة حياة أصول تقنية المعلومات؟

١٨. ما اهتمامات أمن المعلومات خلال مرحلة الاستحواذ من دورة حياة أصول تقنية المعلومات؟

١٩. ما اهتمامات أمن المعلومات خلال مرحلة النشر من دورة حياة أصول تقنية المعلومات؟

٢٠. ما اهتمامات أمن المعلومات خلال مرحلة الإدارة من دورة حياة أصول تقنية المعلومات؟

٢١. ما اهتمامات أمن المعلومات خلال مرحلة التقاعد من دورة حياة أصول تقنية المعلومات؟

٢٢.مــا التحديد النمطي لمواصفات النظــام (System Profiling)؟ وكيف يؤثر في أمن المعلومات؟

٢٣.من مالك الأصل؟

٢٤.ما المسؤولية التشغيلية على الأصل؟

٢٥.اعط مثالاً على حالة لا يكون فيها مالك الأصل صاحب مسؤولية تشغيلية؟

أسئلة على نموذج الحالة:

١. ما الأصول المستهدفة من كل من الدودة الحاسوبية ستكسنت (Stuxnet) والفريق الذي يقف خلفها؟

٢. صنّف كلاً من تلك الأصول باستخدام نظام التصنيف المتبع في هذا الفصل.

٣. بناءً على المعلومات الواردة في المقالات المشــار إليها في الحالة، يبدو أن إيران بذلت جهداً كبيراً في تحديد وحماية أصولها في مدينة (نطنز). ما الاحتياطات الإضافية التي يمكن لإيران اتخاذها؟

نشاط التدريب العملي - تحديد أصول المقررات الدراسية:

في هذا القسم سنستعين بوجودك بصفة طالب في هذا المقرر الدراسي.

أجب عن البنود المرقمة أدناه وأرسل إجابتك إلى أستاذ المادة.

تحديد الهدف:

١. ما هدفك لهذا المقرر الدراسي؟ يمكن أن يكون هدفك بســيطاً مثل «الحصول على درجــة النجاح»، كما يمكــن أن يكون هدفك أكــثر دقة كـ «النجــاح في هذا المقرر الدراسي بدرجة ممتاز».

القوى الخارجية في تشكيل الهدف:

٢. هل هناك قوى خارجية تعمل على تشكيل هدفك لهذا المقرر الدراسي؟ على سبيل المثال:

- هل لديك منحة دراسية تتطلب منك المحافظة على معدل دراسي معين؟ وهذه مشــابهة للقوانــين والتنظيمات التي يجب أن تلتزم بهــا العديد من المنظمات للقيام بالأعمال التجارية.
- هل يساعدك والداك في دفع الرسوم الدراسية، وأنهما طلبا منك عدم حذف أي مقرر دراسي؟ والداك مثل مســاهمي الشركة الذين عليهم التأكد من أدائك في مقابل مستوى هدف معين.
- هــل يجب أن تأخذ هذا المقرر الدراسي وأن تنجح فيه في هذا الفصل الدراسي من أجل التخرج ضمن إطار زمني معين؟

مناقشة واكتشاف الأصول مع زملائك في الصف:

بشكل مشابه لمناقشة عملك مع الآخرين في بيئة العمل فإن التحدث مع زملائك الطلاب قد يؤدي إلى اكتشاف أصول لم تفكر فيها من قبل.

٣. ما الأصول التي تعتقد بأنها تُسهم في تحقيق هدفك؟ وهنا بعض الأمثلة:

- جهاز الحاسب الآلي المحمول.
- أن يقوم أحد ما بإيصالك بالسيارة إلى الكلية يومياً.
- هذا الكتاب الدراسي.
- أستاذك.

حاول التفكير خارج الصندوق للحصول على أشياء غير معروفة لديك حالياً.

تصنيف الأصول:

٤. صنّــف الأصول التي حصلــت عليها كأصول معلوماتية أو أصــول وظيفية أو أصول مكونات الحاسب المادية، أو أصول برمجية أو أصول قانونية.

تسجيل حساسية وأهمية كل أصل:

٥. ما مدى حساسية الأصول التي حصلت عليها؟ وعند الإجابة عن هذا السؤال يجب الأخذ بعين الاعتبار بالنقاط التالية:

- هل هناك مخاطر إذا نظر إليها أحد ما؟
- هل يتم تقييم درجة أدائك في هذا التدريب العملي؟
- ما الذي سيحدث إذا قام شخص ما بنسخ إجاباتك وتسليمها للأستاذ؟
- ما مقدار التأثير في درجاتك في حال فقدان إجابتك وعدم قدرتك على تســليمها في الوقت المحدد؟

ما الذي سيحدث إذا لم تتمكن من القدوم إلى الصف في يوم الاختبار؟

حاول التنبؤ بأسوأ سيناريو عند نظرك في هذه النقاط.

تحديد ملكية وأمين الأصل:

٦. هــل أنت مالك وأمين الأصول التي أدرجتها في القائمة؟ أم أنك، على ســبيل المثال، تستعير جهاز الحاسب الآلي المحمول من شخص آخر؟ هل حقيقة أنك لست مالكاً لـ «أستاذك»؟ وهل تؤثر في هدفك بأي شكل من الأشكال؟

اختر ثلاثة من الأصول واشرح دورة الحياة:

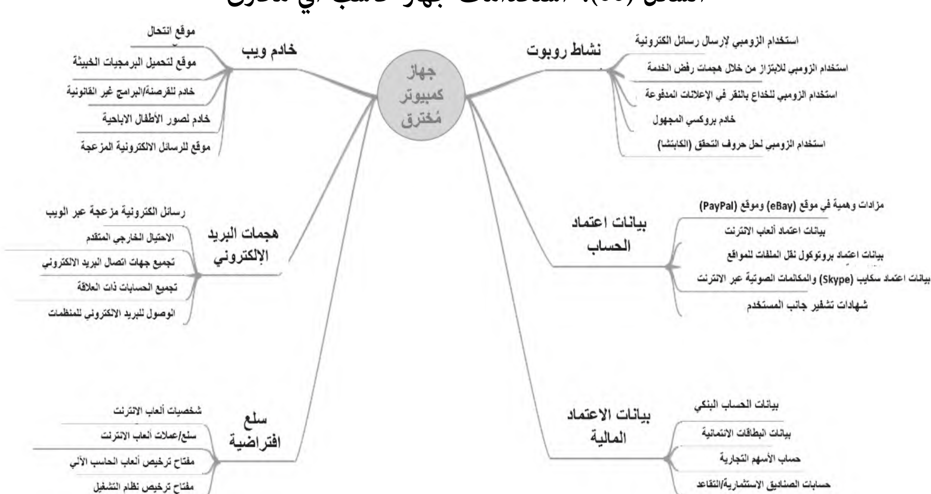
٧. خذ الكتاب الدراسي، على سبيل المثال. كم من التخطيط يشتمل عليه هذا الكتاب؟ هل كانت لديك الفرصة لشراء نســخة مستخدمة من الكتاب؟ هل اشتريت جهاز حاســب آلي محمول خصيصاً لهذا المقرر الدراسي؟ هل ســتقوم ببيعه بعد الانتهاء من هذا المقرر الدراسي؟

٨. في سياق هذا المقرر الدراسي، ما دورة حياة أستاذك؟

تمرين التفكير النقدي - استخدامات جهاز حاسب آلي مُخترق:

لقــد رأينــا في هذا الفصل أن المهاجمين يبحثون دائماً عن طرق للحصول على الســيطرة على جهاز حاســب آلي متصل بشــبكة الإنترنت. وقد حدد بريان كريبس (Brian Krebs)، وهو صاحب مدونة إلكترونية مشهورة بعنوان (krebsonsecurity)، الاستخدامات الممكنة لجهاز حاسب آلي مخترق[١٩] (الشكل ٥-٥).

الشكل (٥٥): استخدامات جهاز حاسب آلي مخترق



أسئلة على تمرين التفكير النقدي:

٩. على فرض أن جهازك الشخصي تم اختراقه، قدّم شرحاً مختصراً لكيفية استخدام الجهاز من قبل المهاجم وذلك لإنجاز ثلاثة أنشطة من تلك الموضحة في الشكل (٥-٥).

تصميم حالة:

لتصميــم الحالــة الأمنية لهذا الفصل، ســنعود لحالــة جامعة ولاية الشــمس المشرقة والمُستخدمة في الفصل الأول والفصل الثاني. إذا كنت تذكر من الفصل الثاني أن عميد شؤون

(19)http://krebsonsecurity.com/wp-content/uploads/2012/07/valueofhackedpc.png

الطــلاب طلب أن نضع مقارنة أوليــة بين الحفاظ على خدمات البريــد الإلكتروني للطلاب داخــل المنظمة، أو اســتخدام (البنية التحتية كخدمــة) (Infrastructure as a Service) لتوفير الدعم لمكونات الأجهزة المادية، أو استخدام حلول (البرمجيات كخدمة) (Software as a Service) من خلال الاستعانة بمصادر خارجية لتأمين الخدمة.

والآن وبعد أن أخذنا نظرة فاحصة على الأصول يمكنك أن ترى شيئاً واحداً بوضوح وهو أنه سيكون هناك تغيير كبير في الأصول اللازمة لدعم كل خيار. وهذه الأصول لا تقتصر على أصول مكونات الحاسب الآلي المادية. فهي تشمل أيضاً الإنشاء المحتمل للأصول المعلوماتية الجديدة مثل التقويمات والوثائق. هل هذه الأصول ستكون داعمة لأهداف الجامعة؟

لتحقيق أهداف هذا التصميم، تأمل في الأصول التالية:

- بيانات البريد الإلكتروني للطلاب.
- برمجيات خادم البريد الإلكتروني.
- المكونات المادية لخادم البريد الإلكتروني.
- التخزين الخارجي.
- اتفاقية صيانة المكونات المادية للخادم.
- صيانة برمجيات خادم البريد الإلكتروني واتفاقية الدعم الفني.
- ٢٠ ساعة عمل أسبوعياً للموظف القائم على دعم الخادم.

ويمكن الاطلاع على وصف للأجهزة الداعمة للبريد الإلكتروني للطلاب من خلال الرجوع إلى تصميم الحالة في نهاية الفصل الثاني. افترض ما يلي:

- مكونات الأجهزة المادية مملوكة بالكامل لإدارة خدمات الطلاب.
- تم شراء برنامج البريد الإلكتروني، ويدعى (Sendmail)، كتطبيق للتعامل مع البريد الإلكتروني الصادر والوارد. وهناك عقد سنوي يغطي تحديثات الصيانة والتصحيحات والدعم الفني.

- يتم تسـعير خدمات (البنية التحتيـة كخدمـة) (Infrastructure as a Service) باسـتخدام معيارين: (١) مقدار عرض النطاق الترددي للشبكة المستخدمة من قبل النظام، و (٢) السعة التخزينية المستخدمة من قبل النظام.
- تم حذف البريد الإلكتروني للطلاب بعد تخرجهم بـ ٧ أيام.

أسئلة على تصميم الحالة الأمنية:

المطلوب منك أن تُسـلم تقريراً جديداً يحتوي على العناصر التالية. وبإمكانك استخدام النموذج أدناه لإدراج الأصول.

الأصل	النوع	الحساسية	الأهمية	داخل الجامعة	بنية تحتية كخدمة (IaaS)	برمجيات كخدمة (SaaS)
بيانات البريد الإلكتروني للطلاب	معلوماتية			x	x	x
برنامج البريد الإلكتروني						
المكونات المادية للخادم						
اتفاقية صيانة المكونات المادية						
التخزين الخارجي						
اتفاقية الدعم الفني لبرنامج البريد الإلكتروني						
ساعات العمل الأسبوعية للموظفين						

١. قـم بتصنيف الأصول الداعمة للبريد الإلكتروني الداخـلي إلى أصول: معلوماتية، أو وظيفية، أو برمجية، أو مكونات الحاسب المادية، أو مالية.

٢. هل بإمكانك تحديد الأصول «الأساسـية» في القائمة؟ ما الأصل المركزي للنظام الذي تقوم بقية الأصول بدعم وجوده؟

٣. في أي مرحلــة من مراحل دورة حيــاة أصول تقنية المعلومــات يعيش خادم البريد الإلكــتروني؟ ما نوع الأصول المطلوبة إذا تم اتخاذ قرار بالاحتفاظ بالبريد الإلكتروني في موقع الجامعة؟

٤. حــدد وبين في التقرير أي هذه الأصول لن يكون هناك حاجة إليه إذا تم نقل البريد الإلكــتروني للطالب إلى حلول البنية التحتية كخدمة (IaaS). وكرر العملية نفســها لحلول البرمجيات كخدمة (SaaS). هل النُسَــخْ الاحتياطية لبيانات البريد الإلكتروني ملائمــة مع حلول البنية التحتية كخدمة (IaaS) وحلول البرمجيات كخدمة (SaaS)؟ ولماذا؟ فكّر في آثار التكلفة.

٥. هل ســيكون هناك منحنــى للتعلم (learning curve) مع اعتــماد النظام الجديد للبريد الإلكتروني خارج الجامعة؟

٦. حدّد وبــيّن في التقرير الأصول «الخفية» التي يكون هنــاك حاجة لها لدعم الضبط الحالي في موقع الجامعة. وكيف تتغير هذه الأصول بالانتقال إلى حلول خارج موقع الجامعة؟ ومن الأمثلة على ذلك ما يلي:

- إذا كان لديك مشــكلة في حساب بريدك الإلكتروني في الجامعة. من الذي تتصل إليه أولاً لحل هذه المشكلة؟
- كيف تنتقل رسالة البريد الإلكتروني من المُرسل وتصل إلى المُستقبل؟
- إذا قام الطالب بالخطأ بحذف صندوق البريد الوارد بأكمله. كيف يتم استرداده؟

٧. قم بتصنيف الأصول وفقاً لوجهة نظرك بالنسبة لحساسيتها وحرجيتها. علل إجابتك.

٨. هــل هناك فــرق في الأهمية بين صناديــق البريد الإلكتروني لمجموعــة مختلفة من الطلاب؟

٩. ناقش في هذا التقرير الوقت المحتمل للانتقال إلى حلول خارج موقع الجامعة.

الفصل السادس

التهديدات والثغرات الأمنية

نظرة عامة:

بعــد الفصول الأولية التي قدمت لمحة عامة عن مجال المخاطر، ألقينا في الفصل الرابع نظرة أولية على مكونات مشــهد أمن المعلومات - الأصــول والتهديدات والثغرات الأمنية، والضوابــط. ثــم بدأنا بأخذ نظرة أعمق على هذه المكونات. وفي الفصل الخامس ناقشــنا موضوع الأصول متضمناً ذلك أنواع الأصول وتصنيفاتها والتعرف على خصائصها.

وفي هذا الفصل سوف نلقي نظرة فاحصة على التهديدات بحيث يجب أن يكون لديك في نهاية هذا الفصل فهم واضح لجوانب المختلفة من التهديدات بما في ذلك:

- نماذج التهديدات، ودمج مكونات التهديد.
- القوى التي يمكن أن تؤثر في الأصل (الوسطاء).
- الطرق التي من خلالها يستطيع الوسطاء أن يؤثروا في الأصل (الأنشطة).
- الثغرات الأمنية وعلاقتها بالتهديدات.

مقدمة:

عرّفنا التهديدات بأنها قدرات الخصوم ونواياهم وأســاليب هجومهم لاستغلال الأصول أو إحــداث ضرر فيها. وهــذا التعريف يتفق مــع تعريف التهديدات الصــادر عن إدارة مخاطــر تقنية المعلومات (NIST SP800-30) والذي ينص على أن التهديد هو «أي ظرف أو حدث من المحتمل أن يؤثر ســلباً في العمليات التنظيمية والأصول، والأفراد، والمنظمات الأخرى أو يؤثر ســلباً في الدولة من خلال نظــام المعلومات عن طريق الوصول غير المصرح به أو تدمير أو إفشــاء أو تعديل المعلومــات و/أو الحرمان من الخدمة»[1]. وبعد أن تقوم

---

(1) http://csrc.nist.gov/publications/nistpubs/800 -30-rev1/sp800_30_r1.pdf، في حين أن هذا التعريف أكثر شمولاً، نعتقد أن تعريفنا للتهديد أسهل للتذكر ويغطي العناصر الأساسية للتهديد.

المنظمة بتحديد أصولهــا والتعرف على خصائص تلك الأصول فإن الخطوة التالية في تحليل متطلبــات أمن المعلومات هي تحليل التهديدات التــي تواجهها المنظمة. ورأينا في الفصل الأخير أن الكثير من أنشطتنا اليومية تعتمد على توافر الأصول، ورأينا كيف أننا نتعامل مع الأصول بأنها من الأمور المُســلَم بها. ما الذي ســيحدث إذا لم نتمكن فجأة من الوصول إلى تلك الأصول؟

وبوصفك محلل أمن معلومات، ســيجري سؤالك بشــكل دوري عن أهمية التهديدات المُســتجدة. هل حقيقة أن شركة مايكروســوفت اكتشــفت أن برنامج إنترنت إكســبلورر (Internet Explorer) مُعــرض لهجــمات البرمجــة النصية للمواقع الإلكترونية المشــتركة (cross-site scripting) تجعلــك تُقــرر بــأن ذلك تهديــداً خطراً بما فيــه الكفاية للقيام بالتحديث الاجباري لجميع أجهزة الحاســب الآلي في المنظمة خلال الأربع وعشرين ســاعة القادمة؟ وهذا شبيه لقرار سكان ولاية فلوريدا الذي يجب أن يتخذوه في كل مرة يقرؤون فيها عن إعصار قادم من المحيط الأطلسي - هل التهديد في هذه المرة خطير بما يكفي لشراء مولد كهربائي لاستخدامه في حال تعطل الطاقة لفترة طويلة؟

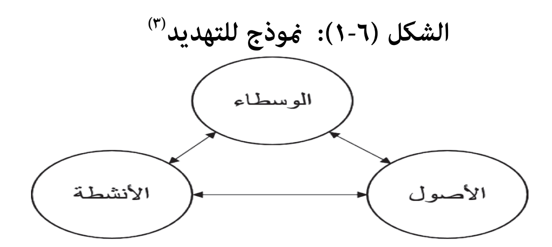
نماذج التهديدات:

تنشــأ التهديدات من أشخاص لهم دوافع (الوســطاء) للقيام بأنشطة محددة لاستغلال الأصول. إن التفاعل بين الوسطاء والأنشطة والأصول ذوي العلاقة يُمثل نموذج التهديد الذي يواجه المنظمة. وهذا التفاعل موضح في الشــكل (٦-١). وفي بقية هذا الفصل سنســتخدم جــزءاً من نموذج تصنيف الحوادث المعروف بــــ (VERIS)[٢]، وهو الجزء الذي يتعامل مع التهديدات بوصفها أساساً للمناقشة في هذا الفصل. وبينما يعتمد بعض الوسطاء والأنشطة في هذا الفصل على نموذج (VERIS) فإن فكرة كون التهديدات أنشــطة للوســطاء بهدف التأثير في الأصول هي فكرة عامة إلى حد ما. وقد سبق أن ناقشنا موضوع الأصول. وفي هذا الفصل نركز على العناصر المتبقية من التهديد وهي: الوسطاء والأنشطة.

---

(٢) نموذج شركة فيريزون لمقاييس مشاركة الحوادث والمخاطر (Verizon enterprise risk and incident sharing metrics framework). ويتضمن هذا النموذج عنصراً رابعاً يشرح كيفية تأثر الأصول. ويتم دراسة نتائج التهديدات كجزء من تحليل المخاطر والتي سنقوم بمناقشتها في فصل إدارة المخاطر.

الشكل (٦-١): نموذج للتهديد[٣]



نموذج التهديد (STRIDE) من مايكروسوفت[٣]

يُعد نموذج (VERIS) واحداً من النماذج العديدة التي يمكن أن تساعد في تصنيف التهديدات. وبالمثل فإن نموذج (STRIDE) أحد النماذج المستخدمة في تصنيف التهديدات، وقد سمي باسم الفئات الست المستخدمة في تصنيف تهديد معين.

انتحال الهوية (Spoofing identity): وأحد أمثلة انتحال الهوية هو الوصول غير المشروع للنظام واستخدام معلومات الاعتماد لمستخدم آخر مثل اسم المستخدم وكلمة المرور.

العبث بالبيانات (Tampering with data): وينطوي العبث بالبيانات على التعديلات الخبيثة في البيانات. ومن الأمثلة على ذلك التغييرات غير المصرح بها على البيانات الثابتة، مثل تلك الموجودة في قاعدة البيانات، وتغيير البيانات التي تنتقل بين أجهزة الحاسب الآلي عبر شبكة مفتوحة مثل الإنترنت.

التنصل (Repudiation): ترتبط تهديدات التنصل بالمستخدمين الذين ينفون تنفيذهم لنشاط معين دون وجود وسيلة لإثبات خلاف ذلك لدى الأطراف الأخرى-على سبيل المثال، مستخدم يقوم بإجراء نشاط غير قانوني على نظام يفتقر لقدرة تتبع العمليات المحظورة. ويشير عدم التنصل (Non-repudiation) إلى قدرة النظام على مواجهة تهديدات التنصل. مثلاً شراء المستخدمٍ لغرض ما قد يستوجب التوقيع على إيصال الاستلام. ويمكن للمورد استخدام الايصال المُوقَع ليكون دليلاً على أن المستخدم استلم المشتريات.

الإفصاح عن المعلومات (Information disclosure): وتتضمن تهديدات الإفصاح عن المعلومات انكشاف المعلومات إلى أشخاص يُفترض ألا يكون لديهم وصول لتلك المعلومات - على سبيل المثال، قدرة المستخدمين على قراءة ملف ما بحيث لم يُمنح لهم حق الوصول لهذا الملف، أو قدرة المتسلل على قراءة البيانات المنتقلة بين جهازي حاسب آلي.

رفض الخدمة (Denial of service): وتجبر هجمات رفض الخدمة النظام على رفض تقديم الخدمة إلى مستخدمين حقيقيين - على سبيل المثال، جعل خادم الشبكة غير متوفر أو صالح للاستخدام مؤقتاً. ويجب الحماية ضد أنواع معينة من هجمات رفض الخدمة وذلك لتحسين الجاهزية والاعتمادية.

رفع الامتيازات (Elevation of privilege): وفي هذا النوع من التهديد يحصل المستخدم الذي لا يملك امتيازات الوصول إلى النظام على تلك الامتيازات ومن ثم يكون لديه حق الوصول لاختراق أو تدمير النظام بأكمله. وتتضمن تهديدات رفع الامتيازات تلك الحالات التي يتمكن فيها المهاجم من الاختراق الفعال لجميع دفاعات النظام، ويصبح جزءاً من النظام الموثوق نفسه، وهذا وضع خطير حقاً.

(٣) نموذج التهديد (STRIDE)-شركة مايكروسوفت: البرمجيات. تم استرجاع النموذج من الموقع الإلكتروني التالي: https://msdn.microsoft.com/en-us/library/ee823878(v=CS.20).aspx

ويُعــد نموذج (VERIS) نموذجاً عاماً يســمح لأي تهديد، بما في ذلك التهديدات التي لم تُكتشــف بعد، ليكون ضمن هذا النموذج. وينسجم النموذج أيضاً مع الأدبيات الأكاديمية حول هذا الموضوع وكذلك مع نماذج المخاطر القياسية التي أخذناها بعين الاعتبار لاحقاً في هذا الكتاب. ومن هنا تأتي أهمية استخدام نموذج التهديد (VERIS).

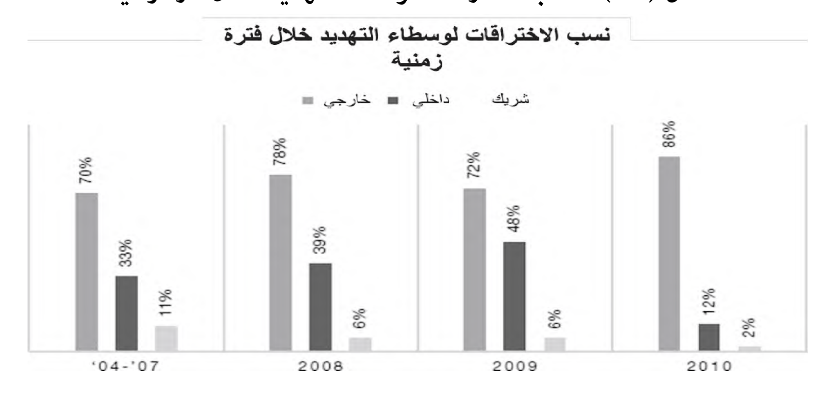
وسيط التهديد:

وسيط التهديد هو فرد أو منظمة أو مجموعة تقوم بتأسيس نشاط تهديد معين. ويمكن تصنيف وســطاء التهديد إلى ثلاثة أنــواع مختلفة، ولكل منها دوافــع مختلفة للمبادرة في تأسيس التهديد.

- الوسطاء الخارجيون.
- الوسطاء الداخليون.
- الشركاء.

الشــكل (٦-٢) يوضح تكرار الفئات المختلفة لوســطاء التهديدات حسب تصنيف نظام (VERIS) منذ نشــأته عام ٢٠٠٤[٤]. ومن الواضح أن عدد الهجمات الداخلية قد انخفض بشكل كبير منذ عام ٢٠٠٩، في حين زاد عدد الوسطاء الخارجيين خلال الفترة نفسها.

الشكل (٦-٢): نسب الاختراقات لوسطاء التهديد خلال فترة زمنية



(٤) لا يصل مجموع الأرقام إلى ١٠٠ لأن العديد من الحوادث لديها أكثر من نوع واحد من الوسطاء.

الوسطاء الخارجيون:

كما يوحي المُسـمى فإن الوسـطاء الخارجيين هم وسطاء خارج المنظمة ولا تربطهم أي صلة بالمنظمة نفسـها. ووفقاً لتقرير خرق البيانات[5] لـ (VERIS) لعام ٢٠١٢ فإن (٩٨٪) من الهجمات في عام ٢٠١٢ نشـأت من وسـطاء خارجيين. وسـنناقش الوسطاء الخارجيين المهمين في القسم التالي. ويوضح الشكل (٦-٣) قائمة سريعة للوسطاء الخارجيين.

الشكل (٦-٣): الوسطاء الخارجيون

الوسطاء الخارجيون
- مجموعات الناشطين
- الحكومات الأجنبية
- الجرائم الالكترونية
- المجموعات المنظمة
- المنافسون
- العملاء
- العوامل الطبيعية وفشل البنية التحتية
- الموظفون السابقون

مجموعات الناشطين:

أصبحـت مجموعة (المجهول) منتشرة في السـنوات القليلة الماضيـة باعتبارها منظمة «اختراق سياسـية» (hacktivist)، وهذه المجموعة تخلط بين النشـاط السـياسي وأنشطة

(5) http://www.verizonenterprise.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf

قرصنــة المعلومــات. وتتكــون مجموعة (المجهول) مــن قراصنة المعلومــات وغيرهم من المتحمسين للإنترنت، وهم أعضاء مجهولون يصورون أنفسهم على أنهم يعارضون كل أنواع القمع الموجودة، كما يعارضون رقابة الجهات الحكومية على الإنترنت في جميع أنحاء العالم. وهنا نذكر قائمة مختصرة من آخر الأنشطة الاستغلالية لمجموعة (المجهول).

آخر أنشطة مجموعة (المجهول) الاستغلالية

أغســطس ٢٠١٢: قامت مجموعة مرتبطة بمجموعة (المجهــول) بالإطاحة بعدة مواقع حكومية في أوغنــدا. وقــد تم ذلك احتجاجاً لتعليــق قانون يُعد جائراً لأعضاء مجتمعات المثلية الجنســية في أوغندا. وتركت المجموعة الرسالة التالية: «ستواصل مجموعة (المجهول) استهداف المواقع الإلكترونية الحكوميــة والاتصــالات في أوغندا حتــى تُعامل الحكومــة الأوغندية جميع الناس بمــا فيهم المثليين بالمساواة».

سبتمبر ٢٠١٢: ادعت مجموعة (المجهول) فصل خوادم اسم المجال (Domain Name Servers) التابعة لشركة (GoDaddy) مما أثر في العديد من الشركات، بدءاً من المواقع الإلكترونية للمجتمعات الصغــيرة ووصولاً للمنظمات الكبــيرة مثل شركــة (JHilI's Staffing Services) وهي شركة توظيف مهنية استشارية.

أكتوبــر ٢٠١٢: هــددت مجموعــة (المجهــول) بملاحقة أهــداف في الســويد رداً على هجمات مــزود خدمات الإنترنــت (PRQ)، وهي الشركة المضيفــة لموقــع (Pirate Bay) وموقع ويكيليكس (Wikileaks).

الحكومات الأجنبية:

وفقــاً للتقريــر الصادر عن مكتب مكافحة التجســس الوطني في شــهر أكتوبر من عام ٢٠١١ [٦] فإن «المعلومات الاقتصادية والتقنية الأمريكية الحساسة مُستهدفة من قبل أجهزة المخابــرات وشركات القطــاع الخاص والمؤسســات الأكاديمية والبحثيــة، ومواطني عشرات الدول». وتضمنت إحدى الحوادث التي حظيت بتغطية إعلامية الاشــتباه بسرقة تصاميم طائرات عسكرية (الشكل ٦-٤ والشكل ٦-٥).

(6) http://www.ncix.gov/publications/reports/fecie_all/Foreign_Economic_Collection_2011.pdf

الشكل (٦-٤): الطائرة العسكرية الصينية (J-20)



الشكل (٦-٥): الطائرة الحربية (F-22) المصممة من شركة لوكهيد الأمريكية



ووفقا للتقرير فإن الصين تأتي على رأس القائمة وذلك للهجوم المتكرر للقراصنة الصينيين على شركات القطاع الخاص الأمريكية. وتجري الاستخبارات الروسية أيضاً نشاط تجسس إلكتروني ضد أهداف أمريكية وذلك لجمع المعلومات الاقتصادية والتكنولوجية.

تقرير شركة (Mandiant) للتحليل الأمني بخصوص وحدة جيش التحرير الشعبي الصيني

في الثامن عشر من شهر فبراير من عام ٢٠١٣ أصدرت شركة التحليل الأمني (Mandiant) تقريراً يبين وحدة من جيش التحرير الشعبي الصيني (Chinese People's Liberation Army) والتي تدعى (APT1) بأنها مصدر لبعض أكثر الهجمات الإلكترونية ضرراً على الحكومة الإلكترونية وشبكات الشركات. ودلت تحقيقات شركة (Mandiant) بأن وحدة (APT1) كانت تعمل منذ عام ٢٠٠٦ وأنها استهدفت مجموعة واسعة من الأهداف.

وفي وقت التقرير قامت شركة (Mandiant) بتحليل اختراقات وحدة (APT1) ضد ما يقارب من ١٥٠ من الضحايا. وكانت شركة (Mandiant) قادرة على تأكيد أن وحدة (APT1) تقع في مدينة شنغهاي، كما كانت قادرة على التعرف على عناصر مختلفة من أدوات تلك الوحدة وتكتيكاتها وإجراءاتها. وكشف التقرير عن ثلاث من الهويات داخل وحدة (APT1) وذلك لإقناع القُراء أن هذه الوحدة تُدار من قبل أشخاص وليس من قبل روبوتات إلكترونية. وتعتقد شركة (Mandiant) أن تلك الهويات تتبع لجنود ينفذون الأوامر المُعطاة لهم من قبل رؤسائهم.

وبناءً على وجود التنظيم لأكثر من ٧ سنوات تعتقد شركة (Mandiant) أن وحدة (APT1) هي كيان ترعاه الحكومة الصينية وتحظى بدعم مباشر منها. وتشير التحقيقات كذلك إلى أن الوحدة رقم (٦١٣٩٨) والتابعة لجيش التحرير الشعبي الصيني يُمكن أن تكون نفسها وحدة (APT١) نظراً للتشابه في المواقع بين وحدة رقم (٦١٣٩٨) ووحدة (APT1). وتُشير تقارير (Mandiant) إلى أن مقر الوحدة يقع في مبنى مساحته (١٣٠,٦٦٣) قدم مربع ويتكون من ١٢ طابقاً وبُني في عام ٢٠٠٧.

وقد حددت شركة (Mandiant) ١٤١ شركة في ٢٠ صناعة رئيسية تم اختراقها من قبل وحدة (APT1). وقامت وحدة (APT1) بسرقة كميات كبيرة من بيانات الملكية الفكرية الثمينة من الشركات التي اخترقتها، كما قامت بتتبع شبكات تلك الشركات على مدى عدة سنوات. وبلغ متوسط مدة الهجوم ٣٥٦ يوماً حيث استمر أطول هجوم تم رصده لمدة ١٧٦٤ يوماً بما يعادل أربع سنوات وعشرة أشهر. ويبدو أن تركيز وحدة (APT1) كان على سرقة الملكية الفكرية بما في ذلك المخططات التقنية وعمليات التصنيع وخطط العمل. وفي حالة واحدة لاحظت شركة (APT1) أن وحدة (APT1) قامت بسرقة ٦,٥ تيرابايت من البيانات المضغوطة من منظمة واحدة وذلك على مدى فترة زمنية بلغت ١٠ أشهر. وتستهدف وحدة (APT1) الشركات التي تنتمي للصناعات التي حددتها الصين بأنها إستراتيجية لنمو الدولة.

وتتطلب وحدة (APT1) أن يتم تدريب موظفيها على أمن الحاسب الآلي وأن يكونوا ماهرين في اللغة الإنجليزية. وتوظف هذه الوحدة بشكل كبير من كليات العلوم والهندسة من المعاهد والجامعات مثل معهد هاربين للتقنية (Harbin Institute of Technology) وجامعة تشجيانغ لعلوم الحاسب الآلي والتقنية (Zhejiang University School of Computer Science and Technology).

ولكن هذا ليس كل ما في الأمر. فحلفاء الولايات المتحدة وشركاؤها يستخدمون إمكانية وصولهم إلى مؤسسات الولايات المتحدة الأمريكية للوصول إلى المعلومات، وذلك باستخدام العديد من أنشـطة التهديد. وتُقدر خسـائر التجسـس الاقتصادي على نطاق واسع قد لا يكون له أي معنى لتتراوح الخسائر بين ٢ مليار إلى ٤٠٠ مليار دولار أو أكثر في العام الواحد.

التجسس الصناعي

في شهر ديسمبر من عام ٢٠١٠ حُكم على ديفيد ين لي (David Yen Lee) بالسجن لمدة ١٥ شهراً، كما أمر بدفع أكثر من ٣٠ ألف دولار تعويضاً لشركة (Valspar)، وهي شركة لصناعة الدهانات والطلاءات الصناعية. كان ديفيد ين لي المدير الفني السابق لتطوير المنتجات الجديدة لمجموعة (Valspar) المعمارية، وقدم استقالته من الشركة بعد عودته من رحلة إلى الصين. وعندما قام موظفو شركة (Valspar) بفحص الحاسب الآلي المحمول وجهاز البلاك بيري التابعة للشركة والتي أعادها (لي) بعد استقالته، لاحظ الموظفون آثاراً لأنشطة تشير إلى أن (لي) كان يحاول تغطية تحركات استخدامه لجهاز الحاسب الآلي المحمول. وكشف الفحص الدقيق لتلك الأجهزة إلى أن الأسرار التجارية لشركة (Valspar) قد تم تحميلها على جهاز الحاسب المحمول.

ويأتي التدخل الحكومي على نطاق واسع ولا يقتصر على الهجمات ضد الولايات المتحدة حيث تشـارك الحكومة الأمريكية أيضـا في الحرب الإلكترونية. وتدعـي صحيفة نيويورك تايمز[٧] أن الرئيس أوباما أمر سراً بزيادة الهجمات الإلكترونية ضد البنية التحتية الحاسوبية للمنشـآت النووية الإيرانية وذلك بعد أسـابيع من توليه منصبه. كما يزعم التقرير نفسه أن الولايات المتحدة وإسرائيل شـاركتا في نشر دودة ستكسـنت (Stuxnet)، والتي أدت إلى الإيقاف المؤقت لـ (٢٠٪) من أجهزة الطرد المركزي العاملة في المنشآت الإيرانية.

(7) http://www.nytimes.com/2012/06/01/world/middleeast/obama-ordered-wave-of-cyberattacks-against-iran.html

خطة (X) لوكالة دفاع مشاريع البحوث المتقدمة

في عام ١٩٥٨ تأسست وكالة دفاع مشاريع البحوث المتقدمة (Defense Advanced Research Projects Agency) لمنع عنصر المباغتة الإستراتيجي من التأثير سلباً في الأمن القومي الأميركي، ولخلق مفاجآت استراتيجية لخصوم الولايات المتحدة من خلال الحفاظ على التفوق العسكري التقني للولايات المتحدة. وفي الآونة الأخيرة، أصدرت وكالة دفاع مشاريع البحوث المتقدمة معلومات عن بدء «خطة إكس» (Plan X). ووفقاً للوكالة فإنها تسعى لبحوث مبتكرة في أربعة مجالات رئيسية لدعم خطة إكس. وقد يرغب الكثير منكم في اتباع هذه التوجيهات لما لها من تأثير في خطط التوظيف في العديد من المؤسسات العسكرية والمؤسسات التابعة لوزارة الدفاع:

فهم معارك الإنترنت: ويركز هذا المجال على تطوير تقنيات التحليل الآلي لمساعدة المشغل البشري في التخطيط للعمليات الإلكترونية. وعلى وجه التحديد يهتم هذا المجال بتحليل خصائص المخطط المنطقي لشبكات النطاق الواسع المتعلقة بنقاط التوصيل (على سبيل المثال، عدد الطرفيات، والروابط النشطة في مقابل الروابط الثابتة، والاستخدام) والطرفيات (مثل زمن الوصول، وعرض النطاق الترددي، وتوالي الدورات).

بناء عمليات إلكترونية يمكن التحقق منها وقابلة للقياس تلقائياً: ويركز هذا المجال على تطوير خطط ذات مهام واضحة على مستوى الإدارة العليا، كما يركز على الادخال الآلي لرسالة النص البرمجي والتي يمكن تنفيذها من خلال واجهة نموذج التفاعل البشري بشكل مشابه لوظيفة الطيار الآلي في الطائرات الحديثة. وهذه العملية ستزيد من فعالية الطرق الرسمية لتحديد خسائر المعركة المحتملة من كل خطة رسالية تم إدخالها.

تطوير نظم ومنصات تشغيل مصممة للعمل في بيئات شبكة ديناميكية ومتنازع عليها ومعادية:

ويركز هذا المجال على بناء «وحدات معركة» صلبة يمكنها أداء وظائف الحرب الإلكترونية مثل رصد أضرار المعركة، وتناوب الاتصالات، ونشر الأسلحة، والدفاع التكيفي.

تصور المعارك الإلكترونية ذات النطاق الواسع والتفاعل معها: ويركز هذا المجال على تطوير وجهات نظر بديهية وخبرة عامة للمستخدم. وتعمل وجهات النظر المُنسقة للمعارك بتوفير وظائف الحرب الإلكترونية مثل التخطيط والتشغيل والوعي الموقفي والمناورات العسكرية.

الجرائم الإلكترونية:

في أواخر التسـعينيات عندما كانت الإنترنت التجارية في مهدها، كان قراصنة الحاسـب الآلي في المقام الأول كـ «أطفال البرامج النصية»، وهم أشـخاص في سـن المراهقة، ووجدوا برنامجـاً نصيـاً في مكان ما وقرروا تشـويه صفحـة على الإنترنت فقط لإظهـار أن قراصنة الحاسـب الآلي قادرون على تعديل بيانات شـبكة الإنترنت. وقـد دمرت العديد من هذه البرامج النصية بيانات الأجهزة المصابة بشكل لا مسؤول وذلك لإثبات هذا المفهوم فقط.

وبعـد فترة مـن العمل المتواصل أصبح طفـل البرامج النصية ذكياً. لمـاذا تقوم بتدمير الأجهزة بينما يمكنك كسـب المال من مسـتخدم هذا الجهاز؟ لماذا تقوم باستبدال صفحة الشـبكة في حين يمكنك الجلوس في المنزل ومراقبة كل الأنشـطة حتى ترى شـيئاً يعجبك؟ والآن ندخل إلى ما يُسمى بالجرائم الإلكترونية. إن الجرائم الإلكترونية تجارة مربحة بشكل لا يصـدق، فيهـا أرباح عالية مع انخفـاض احتمال التعرف على الهويـة ومن ثم المحاكمة مقارنة بالجرائم التقليدية مثل عمليات السطو على البنوك.

ويُعـد «الغش الإلكتروني النيجيري» (Nigerian Scam)، أحد أشـهر وسـطاء التهديد للجرائـم الإلكترونية. ويُعرف الغش الإلكتروني النيجيري بـ (Nigerian Scam 419) وذلك إشـارة إلى مادة في القانون الجنائي النيجـري للتعامل مع الغش. وفيما يلي مثال على بريد إلكتروني للغش النيجري.

لاغوس، نيجيريا.

عناية: الرئيس / المدير التنفيذي

سيدى العزيز،

عرض عمل سري

بعد التشاور مع زملائي، واستناداً إلى المعلومات التي تم جمعها من غرف التجارة والصناعة النيجيرية، أفيدكم بأنه لدي صلاحية طلب مساعدتكم لنقل مبلغ ٤٧،٥٠٠،٠٠٠،٠٠ $ (سبعة وأربعون مليون وخمس مئة ألف دولار أمريكي) إلى الحسابات البنكية الخاصة بك. المبلغ المذكور نتج عن عقد وعن عمولة منفذة دفعت على مدار خمس سنوات من قبل مقاول أجنبي. وكان هذا العمل متعمداً حيث ظل المبلغ من ذلك الحين في حساب بنكي مُعلق في البنك المركزي النجيري (APEX BANK).

نحن الآن على استعداد لتحويل الأموال إلى الخارج وهنا يأتي دورك. ومن المهم أن أحيطكم علماً بأننا ممنوعون من فتح حسابات أجنبية لأننا موظفون مدنيون، ولهذا السبب نحتاج مساعدتك. وسيتم تقاسم المبلغ الإجمالي على النحو التالي: ٧٠٪ لنا، ٢٥٪ لك، و٥٪ لتكاليف حوادث التحويل المحلي والدولي.

وهذا التحويل خالٍ من المخاطر على كلا الجانبين. أنا محاسب لدى مؤسسة النفط الوطنية النيجيرية (Nigerian National Petroleum Corporation). إذا وجدت هذا العرض مقبولاً، نحتاج منك إلى الوثائق التالية:

اسم المصرف، رقم الهاتف، ورقم الحساب، ورقم الفاكس.

أرقام الهاتف والفاكس الخاصة بك - للسرية ولسهولة التواصل.

رسالة منك مختومة وموقعة.

وبدلاً من لذلك سنقوم بتزويدك بنص الرسالة المطلوب تحريرها بالإضافة إلى معلومات تفصيلية بخصوص المطلوب منك. وهذا العمل سيستغرق ثلاثين (٣٠) يوماً لإنجازه.

الرجاء الرد بسرعة.

تحياتي

الآلاف من الرسـائل يجري إرسـالها في وقت واحد. وحتماً فإن المحتالين سـيحصلون على بعض الردود.

في نيجيريا خصصت مقاهي الإنترنت عدداً من أنظمتها إلى الأفراد الذين يعتزمون المشاركة في الأنشطة الاحتيالية. ويُعرف هؤلاء المستخدمون بأولاد ياهو (Yahoo Boys)، وذلك لقيامهم بإنشاء حسابات ياهو زائفة لاستخدامها في مخططاتهم.

وتسـتمر جهـود الحكومة لمنع الجرائـم المالية الإلكترونية حيث يتـم في نيجيريا لصق إعلانـات على جدران مقاهي الإنترنت، وذلك لتحذير المسـتخدمين من الاعتقالات الممكنة

للمحتالـين الذين يرسـلون رسـائل البريد الإلكـتروني الاحتيالية. ولكن بشـكل عام تعلّم المستخدمون الإنصات للقول المأثور «إذا كان شيء ما غير معقول، فربما يكون كذلك».

تعريف الجرائم الإلكترونية في الفلبين

أدى قانون الجرائم الإلكترونية الجديد في الفلبين، والذي قد يؤدي بالحكم بالسجن لمدة تصل إلى ١٢ عاماً، إلى غضب المواطنين والجماعات الحقوقية. والهدف المعلن للقانون واسع النطاق هو معالجة العدد الكبير من جرائم الإنترنت، بما في ذلك المواد الإباحية، والقرصنة، وسرقة الهوية، والبريد الإلكتروني غير المرغوب فيه. وجاء هذا القانون رداً من الشخصيات السياسية على الشرطة التي كانت تشكو من عدم وجود المواد القانونية اللازمة لمتابعة الشكاوى.

والمشكلة أن هذا القانون الجديد يتضمن أيضاً حكماً بوضع قانون التشهير الجنائي في البلاد حيز التنفيذ. إن المستخدم الذي ينشر تعليقات على الإنترنت والتي قد تُعد في وقت لاحق بأنها تشهير من قبل المحكمة قد يواجه عقوبة قصوى تصل إلى السجن ١٢ عاماً وغرامة ٢٤,٠٠٠ دولار أمريكي. وبمقارنة التشهير الإلكتروني بالتشهير في وسائل الإعلام فإن الغرامة تصل إلى نصف هذا المبلغ ومدة السجن تصل إلى ٤ سنوات.

وهذا ليس كل شيء. إن قانون الجرائم الإلكترونية سيسمح لوكالات إنفاذ القانون في الفلبين لجمع بيانات ومراقبة جميع الاتصالات الإلكترونية دون الحاجة لأمر قضائي.

المجموعات المنظمة:

تتطلب بعض التهديدات أن يتعاون العديد من الوسـطاء بعضهم مع بعض؛ لأن تنظيم بعـض المجموعـات للجرائم الإلكترونية أمر ملفت للنظر. على سـبيل المثال، هناك مواقع تُنسـق لبيع وشراء المعلومات المُقيـدة مثل بطاقات الائتمان، وأرقـام الضمان الاجتماعي، ومعلومات الحسابات البنكية، وغير ذلك. وعادة ما تقوم تلك المواقع الإلكترونية بتوظيف عدد كبير من الأفراد بحيث يكون لكل فرد واجباته الوظيفية الخاصة.

- المديرون: تشغيل حسابات الضمان ومراقبة العضوية.
- الوسطاء الدوليون: الإشراف على المحتوى وتحكيم النزاعات.
- المراجعون: تقييم جودة منتجات الموردين.
- الموردون: لديهم صلاحية بيع السلع والخدمات على أعضاء المنتدى.
- الأعضاء (المحتالون): شراء السلع.

ومن أجل أن تصبح مورداً عليك أن تقدم مجموعة من أرقام البطاقات الائتمانية إلى أحد المراجعين. ويقوم المراجع بعمليات شرائية باستخدام تلك الأرقام. وإذا كانت البطاقات الائتمانية سارية المفعول فإنه يتم قبولك بصفة مورد (الشكل ٦-٥). وفيما يلي مثال على تقييم أحد الموردين.

نتائج المراجعة: المخازن الموقتة لـ (زومر). خلال ٢٤ ساعة حصلت على مجموعة من ٥٠ مستودعاً....٤١ منها مقبولة و٩ مرفوضة - لكنه وعد باستبدال المستودعات المرفوضة إذا تم إخباره بذلك خلال ٤٨ ساعة. كما قمت باختبار الشراء من متاجر الإنترنت على أربع بطاقات....ثلاث منها مقبولة ٥٠٠ جنيه استرليني، و ١٢٠٠ جنيه استرليني ، و١٨٠٠ جنيه استرليني، بطاقة الائتمان الأمريكية رفضت المنتج: ١٠/٩ الخدمة ١٠/٩,٥.

وأحد الأمثلة على ذلك موقع كاردبلانت (CarderPlanet). وتُعد كاردبلانت منظمة إجرامية تأسست في عام ٢٠٠١ والتي تقوم بتشغيل وصيانة موقع (www.carderplanet.com) من أجل أنشطتها الإجرامية. وبحلول شهر أغسطس من عام ٢٠٠٤ جذب الموقع أكثر من ٧٠٠٠ عضو. وعلى الرغم من أن معظم المشاركات في المنتدى كانت باللغة الروسية، وأن معظم أعضاء كاردبلانت من أوروبا الشرقية وروسيا، إلا أن جزءاً كبيراً من المنتدى يتحدث باللغة الإنجليزية(٨).

وتم إنشاء المنظمة بطريقة مماثلة للمنظمات الاجرامية بأعضاء ذوي رتب عالية، أو «العائلة»، بأسماء مثل العرّاب (Godfather) أو (رئيس جميع الرؤساء) (capo di capi). وتم إغلاق هذه المنظمة في عام ٢٠٠٤ بعد اعتقال بعض كبار أعضائها. ووفقاً لجهاز الخدمة السرية الأمريكي فإن «الشبكة المكونة من مؤسسي كاردبلانت...لا تزال واحدة من المنظمات الأكثر تعقيداً في العالم وذلك فيما يتعلق بالجرائم المالية من خلال الإنترنت. وتم ربط هذه

(٨) كما نشر موقع كاردبلانت إعلانات تفصيلية، ويمكن الاطلاع على نسخة من تلك الإعلانات في موقع (F-Secure):

- https://www.f-secure.com/weblog/archives/planet.swf
- https://www.f-secure.com/weblog/archives/carderplanet.swf
- https://www.f-secure.com/weblog/archives/555.swf

الشــبكة مراراً وتكراراً تقريباً بكل العمليــات المهمة ذات العلاقة باختراق المعلومات المالية والتي تم الإبلاغ عنها إلى مجتمع إنفاذ القانون الدولي»[9].

المنافسون:

يهتم المنافســون دائماً بتحقيق الميزة التنافســية. وهذا صحيح ليس في القطاع الخاص فحســب ولكن أيضاً في السياســة. ففي عــام ٢٠٠٣، تم توزيع مذكــرات داخلية من قادة الأقليــة الديمقراطية إلى وســائل الإعلام الصديقة للحزب الجمهــوري. «في البداية، رفضت الغالبيــة الجمهورية أي تواطؤ للحزب الجمهوري بعد تسريب المذكرات ونشرها. وفَصّلت الوثائق كيف يمكن لأعضاء مجلس الشيوخ الديمقراطيين وضع إستراتيجية لاستشارة جماعات المصالح الخارجية المخصصة لمعارضة بعض المرشــحين القضائيين المحافظين التابعين للرئيس بــوش. ولكن بعد أن انتقلت الشرطة في الأســبوع الماضي، ناقض الســيناتور أورين هاتش (Orrin Hatch) نفسه، وهو الجمهوري عن ولاية يوتا والذي يرأس اللجنة القضائية، حينما أعلن أنه صُدم عندما عرف أن من قام باختراق الملفات الحاســوبية التابع للأقلية عضواً من موظفيه»[10].

العملاء:

ويمكن للعملاء بســهولة أن يكونوا وســطاء سواء داخليين أو خارجيين اعتماداً على رسم المنظمة لحدود الخدمة. مســتخدمي نظام معلومات الطالب، على ســبيل المثال، هم من الطلاب وكذلك الإداريين في الوحدات المختلفة من نظام معلومات الطالب مثل: المساعدات المالية، والحســابات الدائنــة، وغيرها. ويُعرف هؤلاء المســتخدمون عادة بـ «المســتخدم الوظيفي». وكعملاء يحتاج هؤلاء المستخدمون في أوقات معينة لوظائف وامتيازات تمكنهم من أداء أعمالهم بطريقة أســهل إلا أن ذلك قد يضع الجامعة في خطر. على ســبيل المثال، شــخص من إدارة المســاعدات المالية لديــه إمكانية الوصول إلى أرقــام الضمان الاجتماعي الخاصة بالطلاب، لذا قد يميل هذا الشخص إلى بيع قائمة من تلك الأرقام في سوق القراصنة.

(9) https://archives.fbi.gov/archives/atlanta/press-releases/2010/at081110.htm

(10)http://www.nytimes.com/2003/12/05/opinion/partisan-hacking-in-congress.html

العوامل الطبيعية وفشل البنية التحتية:

في الولايـات المتحدة الأمريكية لدينا حرائق بريـة وزلازل في الغرب، وأعاصير في الغرب الأوسـط، وفيضانات وأعاصير على السـاحل الشرقي على امتداد ولايات الخليج. وعملياً لا يوجد منطقة في البلاد آمنة (١٠٠٪). وبالإضافة إلى ذلك التدخل البشري: تسرب الأنابيب، وحرائق المباني المفاجئة، وغيرها. وكل هذه كوارث طبيعية خارجية يمكن أن تؤثر في البنية التحتية لتكنولوجيا الأعمال التجارية. وعندما تفشـل البنية التحتية لتقنية المعلومات فإن الضرر المالي قد يكون كبيراً. وهذا ما حدث مع شركة سـيرز (Sears) في عام ٢٠١٣ «كلف فشل لمدة خمس ساعات في وقت الازدحام بعد عطلة الأعياد شركة سيرز ١,٥٨ مليون دولار مـن الأرباح وفقاً للدعوى القضائية. (بلغت مبيعات سـيرز ١٢,٣ مليار دولار خلال الربع الرابع لكنها خسرت ٤٨٩ مليون دولار). وعملت الخوادم على مولدات كهربائية لمدة ٨ أيام تم خلالها حرق وقود ديزل بتكلفة ١٨٩ ألف دولار»[١١].

الموظفون السابقون:

يمثل الموظف السـاخط نوعاً خطيراً من الوسـطاء لأنه في كثير مـن الأحيان يكون لديه فكـرة عن الأعـمال الداخلية للمنظمة، كما يكون الموظف السـاخط قادراً على اسـتخدام الثغرات المعروفة لديه للوصول إلى النظام والإضرار بالمنظمة.

في شـهر مايـو من عام ٢٠١٣ تم كشـف النقاب عن شـكوى جنائيـة في يوم الخميس في محكمـة اتحادية في المنطقـة الشرقية لمدينة نيويورك تتضمن اتهام مايكل مينيسـيس (Michael Meneses) الـذي اعتُقـل في وقت سـابق من ذلك اليوم في مدينة سـميثتاون بولاية لونغ آيلاند، بتهمة اختراق شـبكة الحاسب الآلي لشركة تقوم بتصنيع إمدادات طاقة الجهد العالي، مما تسبب في خسارة للشركة بأكثر من ٩٠ ألف دولار. «قام بتوظيف مختلف الأسـاليب التقنية المتقدمة لاختراق شـبكة الشركة الضحية وسرقـة بيانات الاعتماد الأمنية لزملائه السـابقين، بما في ذلك كتابة برنامج يسـتولي على بيانات تسـجيل الدخول وكلمات

(11)http://www.chicagobusiness.com/article/20130604/BLOGS11/130609948/the-price-of-failure-data-center-power-outagecost-sears-2-2m-in-profit#ixzz2X4M39BK1

السر. كما أنه استخدم بيانات الاعتماد الأمنية لزميل واحد سابق على الأقل وذلك للوصول إلى الشبكة عن بعد عبر شبكة افتراضية خاصة (virtual private network) وقام بذلك من منزله ومن فندق يقع بالقرب من عمله الجديد، مما أدى إلى إفساد الشبكة»[١٢].

الوسطاء الداخليون:

الوســطاء الداخليون هم الأشخاص الذين لهم صلة بالمنظمة وغالباً ما يكونون موظفين. ويشمل الوسطاء المتوقعون ما يلي: مسؤولي النظم، وموظفي مكتب الدعم الفني، ومطوري البرمجيــات. لكن غيرهم من الأفراد غير المتوقعين، كموظفي النظافة، يمكن أن يكونوا أيضاً وسطاء تهديد (الشكل ٦-٦).

الشكل (٦-٦): الوسطاء الداخليون

الوسطاء الداخليون
مكتب الدعم الفني
الموارد البشرية
خدمات النظافة
المدققون الداخليون
الإدارة العليا

مكتب الدعم الفني (Help Desk):

قد يتم تخصيص بعض الامتيازات لموظفي مكتب الدعم الفني، عن طريق الخطأ أو عن طريق ســوء الاســتخدام، مما قد يؤثر في عمليات المنظمة. وليس من غير المألوف السماح

(12)www.net-security.org/secworld.php?id = 14861

لموظفي مكتب الدعم الفني بإمكانية تغيير كلمات المرور للمســتخدمين، بعد التحقق من هوياتهــم. وهذة الميزة قد تفتح الباب لرشــوة وابتــزاز الموظفين في حال عدم التحقق من تلك الأنشطة.

الموارد البشرية:

تعيــين الموظفين وإنهــاء خدماتهم في المنظمة، والذي يتم التعامــل معه عادة من قبل إدارة الموارد البشرية، يستلزم بعضاً من الأنشطة التي يحتمل أن يكون من ضمنها تخصيص امتيازات جديدة أو ســحبها مــن أنظمة تقنية المعلومات. ويعرف نشــاط إضافة موظف جديــد إلى النظــام بــ (onboarding)، في حين أن حــذف الموظف من النظــام يُعرف بـ (offboarding). وفي حال تنفيذ هذه الأنشطة أوتوماتيكياً فإن العواقب ستكون وخيمة.

ففي عــام ٢٠٠٥ توجب على أحد البنوك المجتمعية الصغيرة في ولاية فلوريدا اســترداد جميع الرســائل الإلكترونية للموظفين من الأشرطــة الاحتياطية، وذلك بعد حدوث خطأ في نظام الموارد البشرية أدى إلى فصل جميع الموظفين، كما أدى إلى إلغاء وصولهم إلى حسابات البريد الإلكتروني.

خدمات النظافة:

تُعد غرف الخوادم ومراكز البيانات منطقة محظورة على أي شــخص ليس هناك حاجة لوجوده في تلك الغرف. لكن ليس كل الخوادم يكون مكانها في غرف الخوادم. ففي البيئة الجامعية ليس من غير المألوف أن تكون الخوادم في المكاتب المشتركة للموظفين دون وجود حماية مادية ودون وجود بديل لتلك الخوادم.

ففــي عــام ٢٠٠٣ لاحظ عامل نظافة في جامعــة جنوب فلوريدا أن أحــد المكاتب كان قذراً قليلاً فقرر أن ينظف الغرفة بالمكنسة الكهربائية. ولإيصال قابس المكنسة الكهربائية قام بفصل القابس الخاص بجهاز مصدر الطاقة غير المنقطعة «UPS» (uninterruptible power supply) ولكنــه لم يقم بتوصيله عندما انتهى من التنظيف. ونفذ جهاز مصدر الطاقة غير المنقطعة مــن الطاقة مما أدى إلى انقطاع خدمة البريد الإلكتروني عن الجامعة إلى اليوم التالي عندما جاء مسؤول النظام إلى المكتب.

المدققون الداخليون:

هناك أصناف مختلفة من المدققين. فبعض منهم مستعد للعمل مع المسؤولين لفهم الأولويات المختلفة، وتخصيص الموارد، وكيف أن عمليات تقنية المعلومات تتلاءم مع الرسالة العامة للمنظمة. البعض الآخر مهتم بالإشارة إلى الفشل الملحوظ في تقنية المعلومات. والبعض الثالث على استعداد تام لمناقشة مخططات قاعدة البيانات وتوجيهات الشبكة، فضلاً عن الوارد النقدي والمساعدات المالية. كما أن البعض في الصناعة ينظر إلى المدققين بأنهم ماهرون وذوو خبرة عامة، ويُضرب به المثل بأنه متعدد المواهب والمهارات، لكن ليس بالضرورة أن يكون متخصصاً في أي منها.

إن الشغل الشاغل للمدققين هو الامتثال للوائح والأنظمة. ويجب أن تكون أنظمة تقنية المعلومات متوافقة مع القوانين المحلية وقوانين الولاية والقوانين الاتحادية. كما يجب أن تضمن اتباع جميع السياسات والإجراءات الرسمية المعتمدة من قبل المنظمة. ومع أخذ ذلك في الاعتبار، من الضروري تأكيد أن الامتثال يختلف عن الأمن. وهذا الفرق الذي قد يُحّول المدقق في بعض الأحيان إلى وسيط تهديد.

على سبيل المثال، افترض أن لدى منظمتك سياسة تنص على «تشفير جميع أرقام بطاقات الهوية للموظفين عند تخزينها إلكترونياً». وافترض من أجل النقاش في هذا المثال أنه يتم تخزين أرقام بطاقات الهوية على خادم قاعدة البيانات بحيث يتم تشغيل هذا الخادم فقط عند الحاجة للبيانات. ويقع مكان هذا الخادم في منشأة يتم مراقبة الوصول إليها، وأنت الشخص الوحيد الذي يملك الوصول إلى ذلك الخادم. قد يكون من وجهة نظرك أن خطر حدوث تسرب للبيانات أو فقدانها صغير جداً. لكن، وكما سنرى في الفصول القادمة، الامتثال التنظيمي والامتثال لقوانين الولاية والقوانين الاتحادية والتي أنشئت بقصد حماية خصوصية المستخدمين تكون ذات هدف منفرد ولا تنظر إلى أمن النظام بأكمله بل تُركز على الجزء الذي تحتاج إلى حمايته. ولذلك فإن أي مدقق داخلياً كان أم خارجياً يُصر على أن البيانات يجب تشفيرها أو يجب تعديل السياسة إذا كانت المنظمة تحتمل المخاطر، حتى إذا كانت المنظمة سوف تضطر إلى إنفاق آلاف الدولارات من أجل تشفير البيانات.

وقد يؤثر المدققون أيضاً في عمليات تقنية المعلومات. ففي ولاية فلوريدا إذا كانت غرفة الخادم لا تتفق مع معايير المباني بسبب استخدام التوصيلات الكهربائية فإنه يحق لرجال الإطفاء قطع التيار الكهربائي على الفور حتى لو تعطلت العمليات الهامة للمنظمة بسبب انقطاع التيار الكهربائي.

الإدارة العليا:

يمكن اعتبار المديرين وسـطاء تهديد من خلال طرق متعددة. ولكن التهديد الأكثر هو عدم دعم الإدارة العليا لتقنية المعلومات بشكل عام وعدم فهم المخاوف الأمنية. إن أنظمة تقنية المعلومات موجودة في كل مكان في المنظمات في الوقت الحاضر، لكن الناس لا تدرك التبعية التي تنشـئها تلك النظم. ففي الجامعة، رواتب أعضاء هيئة التدريس، والتسجيل، وكشـوف الدرجات، والمسـاعدات المالية، كلها تعتمد على حقيقـة أن تتوفر أنظمة تقنية المعلومات وتعمل بشكل صحيح.

ومعظـم تقنية المعلومـات تعمل في عالم «لا خبر يُعد خبراً جيـداً». وبينما يكون ذلك حسـناً من وجهة نظر تشـغيلية إلا أنه يخلق حاجزاً مع المستخدمين. لكن من وجهة نظر المسـتخدم فإنه من الصعب تبرير النفقات المرتبطة بشراء خادم جديد إذا كانت الخدمات مـا زالـت تُقدم دون أي تأثير في الأداء. وعلى المدى الطويل يمكن أن يتسـبب نجاح تقنية المعلومات في فشـل تلك التكنولوجيا، إذا لم يتم تذكير الإدارة باسـتمرار باعتمادية الأعمال على الخدمات التي توفرها تقنية المعلومات.

جامعة جديدة: جامعة فلوريدا المتعددة الفنون (Florida Polytechnic)

في عام ٢٠١٢ وافق مسؤولو ولاية فلوريدا على إنشاء جامعة معتمدة من الولاية اسمها جامعة فلوريدا المتعددة الفنون (Florida Polytechnic) أو (FPU). وكانت هذه الجامعة سابقاً جزءاً من نظام جامعة جنوب فلوريدا. وقد سبّب هذا القرار من قبل حكومة الولاية لإنشاء هذا الكيان الجديد في ظهور تحديات تقنية المعلومات، وهذا يُظهر نموذجاً لقرارات الإدارة العليا التي تؤسس لمشكلات تنتقل آثارها السلبية الممكنة إلى الأمن العام للمنظمة.

يجب مراجعة جميع رخص البرمجيات لأن أجهزة الحاسب الآلي والخوادم تعود ملكيتها الآن للجامعة الجديدة وليس لجامعة جنوب فلوريدا. وقد يؤدي عدم القيام بذلك إلى قضايا قانونية خطيرة.

يجب إعادة تخصيص موظفي تقنية المعلومات لتقديم الدعم ونقل المحتوى من خوادم جامعة جنوب فلوريدا إلى الخوادم الأخرى المملوكة لجماعة فلوريدا المتعددة الفنون، مما يؤدي إلى ترك بعض المناطق بدعم محدود.

وبينما يُنقل بعض الموظفين إلى النظام الجديد فإن العديد من الموظفين يفصلون. وهذا يخلق السيناريو المثالي والمحتمل لموظف ساخط ليصبح وسيط تهديد بارتكاب الغش.

الشركاء:

ويشمل أي طرف ثالث يتقاسم علاقة العمل مع المنظمة. وهذا يشمل الموردين والبائعين ومقدمي الاستضافة، ومقدمي الدعم التقني الخارجيين، وغيرهم. وعادة ما تنطوي العلاقة بين شركاء العمل على مستوى معين من الثقة والامتيازات (الشكل ٦-٧).

الشكل (٦-٧): الشركاء

الشركاء
الخدمات الاستشارية والمقاولون
خدمات الحوسبة السحابية
الموردون

الخدمات الاستشارية والمقاولون:

وتشمل هذه الفئة أيضاً خدمات التركيب والصيانة. وهذه خدمات مدفوعة من قبل المنظمة من أجل أداء وظيفة معينة أو لزيادة الموظفين المحليين.

وتبذل المنظمات الاستشارية قصارى جهدها للامتثال لأي متطلبات خاصة لعملائها. لكن العملاء من ذوي الاحتياجات الخاصة قد يُصدمون إذا كان تدقيق التفاصيل مهماً للغاية بالنسبة لهم. تأمل في قضية التسرب الأمنية التي حدثت مؤخراً في وكالة الأمن القومي (National Security Agency) والتي تورط فيها إدوارد سنودن (Edward Snowden). كان السيد سنودن موظفاً في شركة بوز ألن هاملتون (Booz-Allen Hamilton)، وهي الشركة التي قدمت الكثير من العمل التقني لوكالة الأمن القومي وغيرها من الوكالات الفيدرالية الحساسة.

ففي الفترة الزمنية من ٥ يونيو إلى ٢١ يونيو من عام ٢٠١٣، كشفت صحيفة الجارديان (Guardian) أوامر سرية للغاية بالسماح لوكالة الأمن القومي بجمع معلومات عن

المواطنين الأمريكيـين. وفوجئ مشرعو القانون والجمهور بكشـف صحيفة الجارديان عن هذا الخبر.

وتراوحت ردود الأفعال بين تسـمية السـيد سـنودن بطلاً لتسـليطه الضـوء على تلك الأنشـطة، وبين وصفه بخائن لكشفه عن الإجراءات الأمنية التي حافظت على أمن أمريكا. وفي وقت كتابة هذه السـطور، لم يعرف مصير السـيد سـنودن بعد حيث تعمل الحكومة الأمريكية على جلبه إلى الولايات المتحدة الأمريكية لمحاكمته (الشكل ٦-٨).

لكن من وجهة نظر أمن المعلومات، أدت هذه الحادثة إلى الاهتمام بالعديد من الأمور. فنظراً لطبيعة المنظمة فإنه من المسـتحيل تأكيد كيف قام السـيد سنودن بإخراج البيانات من الشركة حتى تم الكشـف عن ذلك في جلسة المحاكمة، ومن خلال الشهادة الفيدرالية، وبقية الطرق الرسمية الأخرى. لكن كان هناك تخمين بأن السيد سنودن قد استخدم قرص الناقل التسلسـلي العالمي (USB thumb drive) لحفظ بياناته. لكن المنظمات الحساسة تقـوم عادة بتعطيل هذه المنافذ على أجهزة الحاسـب الآلي لمنع هـذا التسرب. لذا تفاجأ العديـد من الخبراء بإمكانية هذه الاحتمال في وكالة الأمن القومي. وجدير بالملاحظة أيضاً كيف أن موظفاً يتبع لشريك (مقاول) قد تمكن من الوصول إلى تلك الوثائق الحساسة.

> في بداية عام ٢٠٠٠ كانت شركة (Sun Microsystems) مسؤولة عن تركيب العديد من أنظمة الأداء العالي في جامعة جنوب فلوريدا. ومن أجل تسهيل عملهم قام مهندسو الصيانة من شركة (Sun Microsystems) بتجهيز جميع الصناديق، بما في ذلك تجهيز صناديق المنظمات الأخرى، بنفس بيانات تسجيل الدخول وكلمات المرور. ومما يُضيف إلى الخلل الأمني هذا أن كلمة المرور كانت مستندة إلى قاموس الكلمات.

خدمات الحوسبة السحابية:

تمثل خدمات الحوسبة السحابية فئة كبيرة جداً من الخدمات. وتحدد إدارة مخاطر تقنية المعلومات (NIST)[١٣] خمس خصائص أساسـية للحوسـبة السحابية: الخدمة الذاتية بناء على الطلب، والوصول إلى الشبكة ذات النطاق الواسع، وتجميع الموارد، والمرونة السريعة أو

(13) http://csrc.nist.gov/publications/PubsSPs.html#800-145

التوسع، والخدمة المُقاسة. كما ذكرت أيضاً ثلاثة من «نماذج الخدمة» (البرمجيات، والمنصة، والبنية التحتيــة)، وأربعة من «نماذج النشر» (الخاص، والمجتمــع، والعام، والهجين) والتي تقوم جميعها بتصنيف طرق تقديم الخدمات السحابية.

الشكل (٦-٨): إدوارد سنودن (Edward Snowden)



وجميع تلك الخدمات كانت في وقت مــن الأوقات مرتبطة بمصطلح (Outsourcing) والــذي يعني (التعاقــد الخارجي). ونظراً لارتباط مصطلــح (Outsourcing) بفقد بعض الأشــخاص لوظائفهم، أعادت الصناعة تصميم نفســها كما أعادت تصنيف الخدمات تحت مسمى «خدمات الحوسبة السحابية».

فعندما تتجه المنظمات لنقل بعض خدماتها للسحابة الإلكترونية فسيكون هناك فرضية لتطوير وجود بديل للأجهزة المستخدمة، وكذلك تطوير الموثوقية مع عدة خوادم تستضيف تطبيقــات بميــزة الانتقال التلقائي في مواقع جغرافية متعــددة. وفي حين أن هذا هو الحال في معظــم الحالات إلا أنه لا يكون كذلك دائماً، لكن يجب على منظمات الأعمال ألا تفترض تلك الفرضية. عندما تنتقل بعض الخدمات إلى الســحابة الإلكترونية، لابد من التحقق من بعض الأمور:

- هل لدى مراكز البيانات الشهادات الأمنية المطلوبة؟
- ما المواقع الجغرافية للمركز؟
- ما الضوابط التي تم وضعها لحماية البيانات؟

ومـن الأهمية بمكان أيضاً أن يكون هناك من البداية إسـتراتيجية للخروج. فلا بد من تأسـيس الطرق التي مـن خلالها يمكن نقل البيانـات إلى موقع آخر في حـالات الطوارئ، فالفشل في أي من هذه النقاط يمكن أن يحول مزود الخدمة الخارجي من شريك إلى وسيط تهديد.

أمثلة على بعض قضايا مزودي خدمات الحوسبة السحابية

شركة (Dropbox):

في شهر يوليو من عام ٢٠١١ قامت شركة تخزين البيانات السحابية (Dropbox) بتغييرات جذرية على اتفاقيات التراخيص والشروط نتيجة لمشكلة سابقة اشتملت على خلل برمجيات في نظام التوثيق. «من خلال إرسالك الملفات إلى الخدمات فإنك تمنحنا، وتمنح الجهات العالمية التي تعمل معها لتقديم الخدمات، الحق في استخدام وتوزيع ونسخ وأعداد أعمال مشتقة (مثل الترجمة وتغييرات في التصميم) وعرض الملفات علانية بالقدر اللازم للخدمة ويكون ذلك الحق غير حصري ودون رسوم وقابلاً للترخيص لطرف ثالث». لكن شركة (Dropbox) غيرت موقفها بسرعة بعد أن بدأ العملاء برفض الاتفاقية وسحب بياناتهم من الشركة.

شركة (Salesforce.com):

وهذه الشركة معروفة ببرمجيات إدارة علاقات العملاء (Customer Relation Management)، وهي معروفة أيضاً بعروض الخدمات السحابية: مبيعات السحابة (Sales Cloud) لإدارة المبيعات، خدمات السحابة (Service Cloud) وهي خدمة مقدمة لمراكز الاتصال.

لكن شركة (Salesforce) لا يوجد لديها مراكز بيانات خاصة بها حيث تتعامل مع شركة تدعى (Equinox) وذلك للاستفادة من هيكلة تُسمى بهيكلة (DR) من أجل الحفاظ على خدماتها.

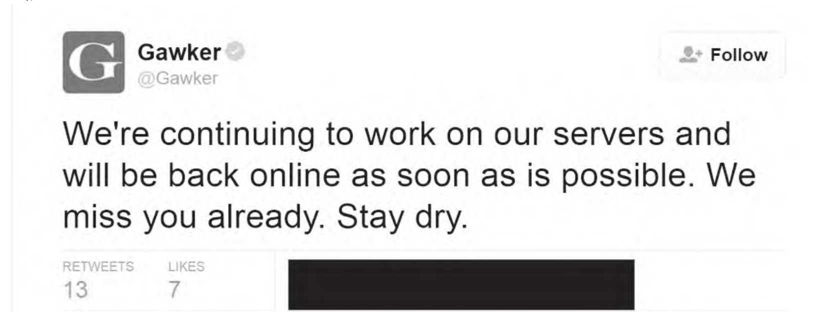
وفي شهر يوليو من عام ٢٠١٢، حدث انقطاع وجيز لمدة دقيقة واحدة في التيار الكهربائي في أحد مواقع مراكز البيانات في كاليفورنيا التابع لشركة (Equinox) مما أدى إلى سلسلة من المشكلات أدت في نهاية المطاف إلى التعطل الكامل لشبكة (Salesforce) لما يقارب من ٦ ساعات.

تُعـد الاسـتعانة بمصدر خارجي لتهيئة البنيـة التحتية لغرفة الخادم أمراً شـائعاً حيث يسـاعد ذلك عـلى التخلص من المخاوف الطبيعية ويسـمح للمنظمـة بالتركيز على الجزء

المهم من أعمالها. وهذا ينطبق بشكل خاص على مدونات المواقع الإخبارية وبعض وسائل الإعلام.

ففي شـهر أكتوبر من عام ٢٠١٢ ضرب إعصار سـاندي السـاحل الشرقي القريب من مدينـة أتلانتيك. اسـتيقظ القُرّاء في اليوم التـالي بخيبة أمل لأن بعـض المواقع الإخبارية المفضلـة لديهم تعطلت عـن العمل بما في ذلـك (The Huffington Post) و(Gawker) حيث كانت المنصة الرئيسـية لمزود خدمة الإنترنت لهذه المواقـع تابعة لـ (Datagram). لقد غمرت مياه الفيضان مراكز البيانات التابعة لـ (Datagram)، وتعطلت خطوط الطاقة التي تغذي المولدات، مما أدى إلى تعطل مركز البيانات بالكامل (الشكل ٦-٩).

الشكل (٦-٩): تعطل مزود خدمة الإنترنت (Datagram) بسبب إعصار ساندي



الموردون والبائعون:

عندما لا يتمكن الباعة أو الموردون من توريد الموارد المطلوبة، أو مراقبة مستوى جودة الأجهـزة، أو تقييم علاقاتها التجارية بشـكل صحيح فإن التأثير على نطاق العمل قد يكون كبيراً.

> في شهر مايو من عام ٢٠١٣ فازت شركة نوكيا (Nokia) بأمر قضائي ضد شركة إتش تي س (HTC) في هولندا وذلك فيما يختص ببيع هاتف أندرويد يُسمى (HTC One). ويظهر أن (HTC) استخدمت ميكروفوناً في هاتف (HTC One) مُطور من شركة (STMicroelectronics)، لكن على ما يبدو أن شركة نوكيا لديها حقوق حصرية لاستخدام هذا الميكروفون في أجهزتها.

نشاط التهديد:

الوسيط هو الجزء الأول من التهديد. لكن لن يكون هناك أي تهديد حتى يقوم الوسيط ببعض الأنشطة للإضرار بأحد الأصول. النشاط هو العمل الذي يقوم به الوسيط للتأثير في خصوصية الأصل أو تكامله أو جاهزيته. إن عملية إنشاء قائمة من الأنشطة غير مجدٍ لأن أنشطة التهديدات الجديدة تكون محدودة فقط بمدى براعة الوسطاء. ومع ذلك يمكن تصنيف أنشطة التهديدات الشائعة في الفئات التالية:

- البرمجيات الخبيثة (Malware).
- قراصنة الحاسب الآلي (Hackers).
- الهندسة الاجتماعية (Social engineering).
- مادي (Physical).
- الأخطاء (Error).
- البيئة (Environment).

البرمجيات الخبيثة (Malware):

مصطلح (Malware) اختصار لـ (malicious software) والتي تعني البرمجيات الخبيثة. وهي البرمجيات التي صُممت خصيصاً للتدمير والتعطيل والسرقة، أو بشكل عام إحداث أنشطة سيئة أو غير شرعية على أجهزة الحاسب الآلي. الفيروسات والدودة الحاسوبية وأحصنة طروادة والروبوتات الشبكية كلها أمثلة على البرمجيات الخبيثة.

وقد ازداد عدد البرمجيات الخبيثة بشكل كبير حيث ارتفع عددها من ١٣٠٠ في عام ١٩٩٠ إلى ٥٠ ألف في عام ٢٠٠٠ وصولاً لأكثر من ٢٠٠ مليون في عام ٢٠١٠.

الفيروسات:

تنتشر الفيروسات بواسطة ملف «مضيف» يتطلب تفاعل بشري لتنشيطه. وقد يكون الملف المصاب موجوداً في القرص الصلب لجهاز الحاسب الآلي، لكن الجهاز لن يكون مصاباً

حتى يتم تشغيل الملف. وينتشر الفيروس عندما يقوم شخص ما بإرسال ذلك الملف المصاب إلى جهاز جديد، ويُشغل ذلك الملف على المضيف الجديد.

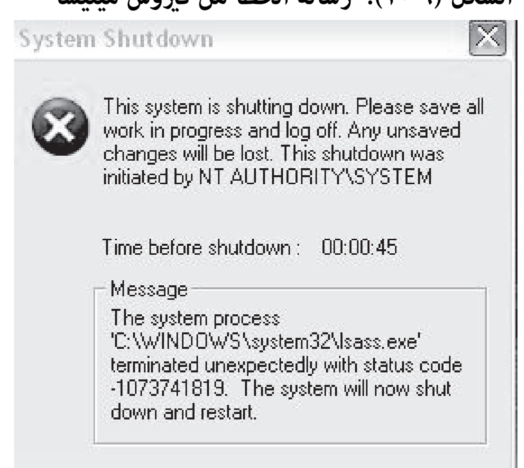
وفي عام ١٩٧١ أنشئ أول جزء برمجي يُعد فيروساً من قبل موظف في شركة تُدعى (BBN)، والتي تسمى الآن (Raytheon BBN). وتقوم شركة (BBN) ببناء تبديل حزم الشبكات (packet switching networks) لـ (ARPANET) والتي تُعد باكورة الإنترنت. وتم تصميم برنامج يدعى (Creeper) لإثبات مفهوم برمجيات التكرار الذاتي حيث يقوم بالقفز من خادم إلى خادم آخر، ويقوم بتنصيب نفسه، ثم يُزيل النسخة السابقة ويُظهر الرسالة التالية على شاشة المضيف الجديد «أنا (Creeper) اقبض عليّ إذا كنت تستطيع ذلك» (I am Creeper, catch me if you can).

ويُعد انتشار فيروس ميليسا (Melissa Virus) أول انتشار لفيروسات تنال من شبكات الشركات. وكان ميليسا مختلفاً عن الفيروسات الأخرى بسبب السرعة التي انتشر بها حيث كان يُخفي نفسه في رسالة بريد إلكتروني بعنوان «رسالة مهمة من <شخص تعرفه>». وكانت الرسالة الإلكترونية تحمل مستند مايكروسوفت وورد يحتوي على فايروس ماكرو (macro virus)، وهو الفيروس الذي يشغل نفسه تلقائياً عند فتح الملف.

الأجهزة المصابة بفيروس ميليسا تعاني من الأعراض التالية:

- إيقاف غير مبرر لتشغيل الجهاز مع رسالة خطأ الموضحة في الشكل (٦-١٠).
- عند فتح وثائق مايكروسوفت وورد يقوم الجهاز المصاب بعرض مقتطفات من حلقات البرنامج التلفزيوني «عائلة سيمبسون».
- يتم اختيار ملفات عشوائية تحتوي على الفيروس لإرسالها عبر البريد الإلكتروني إلى ٥٠ من المستخدمين الموجودين في دفتر عناوين جهاز الحاسب الآلي.

الشكل (٦-١٠): رسالة الخطأ من فيروس ميليسا



وبالإضافة إلى المشكلات التي تركز على المستخدم النهائي، سبّب فيروسا ميليسا مشكلات خطيرة في بنية البريد الإلكتروني التحتية للشركات بسبب الأحمال العالية للأجهزة المصابة والموجهة إلى خوادم البريد الإلكتروني. وتم القبض على مصمم هذا الفيروس وحُكم عليه بالسجن لمدة ٢٠ شهراً وغرامة قدرها ٥ آلاف دولار.

الدودة الحاسوبية:

بينما تعتمد الإصابة بالفيروسات وانتشارها على التدخل البشري، تستخدم دودة الحاسب الآلي ثغرات نظام التشغيل أو التطبيقات للدخول عبر الشبكة واستغلال نقاط الضعف نفسها الموجودة في الأجهزة الأخرى. ودودة موريس (Morris Worm) هي الدودة الحاسوبية الأولى التي ظهرت في عام ١٩٨٨. وعلى الرغم من أن هذه الدودة تشبه فيروس (Creeper) من حيث أن كليهما صُمم لإثبات نظرية ما، لكن بسبب خطأ في كتابة التعليمات البرمجية أصبح للبرنامج فرصة ثابتة في التكاثر وإنتاج نسخ مُتعددة من البرنامج نفسه في الجهاز المصاب مما يؤدي إلى زيادة حمل الجهاز المضيف، وفي نهاية المطاف يؤدي أحياناً إلى تعطل الجهاز المضيف.

وتُعد دودة إس كيو إل سلامر (SQL Slammer worm)، والتي ظهرت في شهر يناير من عام ٢٠٠٣، واحدة من الديدان الحاسـوبية الأسرع انتشاراً في التاريخ، وذلك لأنها استفادت من ثغرة تجاوز سـعة المخزن المؤقـت (buffer overflow) الموجـودة في خادم تعليمات الاسـتعلام البُنيوية (Microsoft SQL Server ٢٠٠٠) لتكرار نفسـها. والعواقب الواضحة للإصابة بدودة سلامر في جميع أنحاء العالم ما يلي:

- عندما انتشر هـذا الفيروس كانت العديد من ماكينات الصرف الآلي لمصرف (Bank of America) غير متوفرة.
- قامت الخطـوط الجوية (Continental Airlines) بإلغاء وتأخير رحلاتها بسـبب إصابة نظام التذاكر بهذه الدودة.
- تعطل نظام الطوارئ (911 system) عن العمل في مدينة سياتل.

والمشـكلة هنا ليسـت الإصابة بالدودة نفسـها بل السرعة المرعبة التـي كانت تحاول الدودة أن تنشر نفسـها. إن إصابة جهاز واحد تؤدي إلى إغراق الشـبكة في غضون دقائق مما يؤدي وبشـكل فعـال إلى خلق هجوم رفض الخدمـة (Denial of Service Attack) باسـتخدام كل النطاق الترددي المتاح للشبكة. وتشير التقديرات إلى أنه تمت إصابة (٩٠٪) من الخوادم ذات الثغرات على الإنترنت في غضون ١٠ دقائق من إطلاق هذه الدودة.

الروبوتات الشبكية (Bots):

أحـد أشـهر الروبوتات الشـبكية التي تم اكتشـافها من قبل قطاع الأمن يُعرف باسـم (ZeroAccess). وتشير التقديرات في شهر سبتمبر من عام ٢٠١٢ إلى أن البرمجيات الخبيثة المعروفة بـ (ZeroAccess) قد جرى تحمليها قرابة ٩ ملايين مرة. والروبوتات الشبكية هي البرمجيات ذات الاسـتخدام العام، وتكون مثل القشور الخارجية الفارغة، التي تتصل بخادم الأوامر والتحكم (Command and Control server) من أجل إصدار أوامرهم. ويستخدم الروبوت الشبكي (ZeroAccess) الشبكات المشابهة لشبكة النظراء (peer-to-peer) لتنزيل الإضافات من خوادم الأوامر والتحكم (Command and Control server). وتقوم هذه الإضافات بتنفيذ المهام المصممة لتوليد الإيرادات لمشـغلي الروبوتات. وتقوم بتنفيذ هذه

المهمة من خلال طريقتين أساسـيتين: احتيال النقـر (Click Fraud)، والتنقيب عن عملة الإنترنت بت كوين (Bitcoin Mining).

ويحـدث احتيال النقـر (Click Fraud) عند الارتباط بالأعمال التي تسـتخدم نموذج الإعلانات المعروف بالدفع حسـب عدد النقرات (Pay Per Click). وبشـكل عام الدوافع تختلف. وعادة ما يتم توظيف قراصنة الحاسـب الآلي في محاولة لتجفيف ميزانية الدعاية للمنافسين. والجناة الأكثر شيوعاً هم الناشرون الذين نجحوا في السابق في إدارة هذا النوع من الاحتيال[١٤].

ويمكن وصف عملة الإنترنت بت كوين (Bitcoin) بأنها العملة الافتراضية الجديدة التي تحل محل النقود في شبكة الإنترنت. وبشكل مشابه للاحتياطي الاتحادي (البنك المركزي في الولايات المتحدة) (Federal Reserve) المسؤول عن تنظيم العملة النقدية فإنه تم تفويض تنظيم عملة البت كوين (Bitcoin) إلى شـبكة النظراء (peer-to-peer) والتي تتألف من أجهـزة حاسـب آلي تعمل عـلى عميل البت كويـن، أو ما يُعرف بـ (تنقيـب البت كوين) (Bitcoin Miner). وعندمـا تقـوم بتثبيت (عميل البت كوين) عـلى جهازك فإن الجهاز يعمل بشكل أساسي كأنه بنك بت كوين (Bitcoin bank) يقوم بإصدار العملة والتأكد من صحة المعاملات وغيرها. ويصبح الأفراد عادة جزءاً من مجموعة التنقيب (mining pool) ويحصلون على تعويضات بت كوين (payout bitcoins) كجزء من سدادهم للمدفوعات. ومن الواضح أن الروبوتات الشبكية مناسبة جداً لهذا النشاط.

القرصنة:

وفقاً لتقرير اختراق البيانات التابع لنموذج تصنيف الحوادث (VERIS) لعام ٢٠١١ فإن (٨١٪) من الخروقات في عام ٢٠١١ قد تضمنت نوعاً من أعمال القرصنة. وبعض الأساليب المسـتخدمة للوصـول إلى الأجهزة تتم من خلال البرمجيات الخبيثة. والفرق الأسـاسي بين اختراق القرصنة وبين الإصابة بالبرمجيات الخبيثة هو أن الإصابة بالبرمجيات الخبيثة تنتشر تلقائياً دون تدخل العنصر البشري. وعلى الرغم أن كلاً منهما قد يستخدم أساليب الاختراق

(14) What is Click Fraud? - Internet Marketing Services By (n.d.). Retrieved from http://www.optimum7.com/internet-marketing/ppc/what-is-click-fraud.html

نفســها، فإن اختراق القرصنة هو هجوم موجه من قبل القرصان ويســتهدف مجموعة أو منظمة معينة.

هجوم القوة الغاشمة (brute-force attack):

هجوم القوة الغاشمة هو الطريقة التي يحاول قراصنة الحاسب من خلالها الوصول إلى حساب على النظام المستهدف، وذلك بمحاولة «تخمين» كلمة المرور الصحيحة. وفي العادة تكون هذه العملية آلية وقد تستغرق ساعات لإكمالها.

وعــلى الرغم من أن إصدارات هذا الهجوم التي «صُنعت للعرض على شاشــة التلفاز»، والتي يحاول فيها القرصان بعضاً من كلمات المرور وبعد ذلك يتمكن بســهولة من الدخول إلى جهاز الحاسب الآلي، إلا أنها ليست بعيدة جداً عن الحقيقة. إن تحليل ٤٥٠ ألف كلمة مــرور تم تسريبها من خلال هجمة على موقع ياهــو، والتي تم ذكرها آنفاً في هذا الفصل، يبرز لنا النقاط الهامة التالية:

- إن كلمة السر لـ ١٦٠ حساب على ياهو هي (١١١١١١).
- تم استخدام كلمة «password» ككلمة مرور في ٧٨٠ مرة.
- تم اســتخدام كلمــة «ninja» ككلمة مــرور في ٣٣٣ مرة (لكن المســتخدم لم يكن كالنينجا الذي أراد أن يكون مثله).

وفيما يلي عينة من كلمات السر غير الملائمة والتي تحتوي على أســوأ ٢٥ كلمة مرور في عام ٢٠١١ (الجدول ٦-١) حيث تم استخراجها من برنامج مكافحة الفيروسات (ESET)[١٥].

هجمات بيانات الاعتماد الافتراضية (Default credentials attacks)

تــأتي الأجهزة مصممة لتكون متصلة عادة من المصنــع بكلمة مرور افتراضية. وينطبق هذا الكلام على بعض التطبيقات البرمجية وقواعد البيانات. وتشير هجمات بيانات الاعتماد الافتراضيــة إلى الحوادث التي يقوم فيها قراصنة الحاســب بالوصول إلى نظام أو إلى برنامج

(15) http://blog.eset.com/2012/06/07/passwords-and-pins-the-worst-choices

محمي بواسطة اسم مستخدم وكلمة مرور موحدة ومحددة مسبقاً (ومن ثم تكون معروفة على نطاق واسع).

وهناك العديد من المواقـع الإلكترونية التي تقوم بجمع قوائم كلمات السر الافتراضية. موقع (CIRT.net)، على سـبيل المثال، يحتفظ بقاعدة بيانـات تتضمن ١٩٣٧ كلمة مرور افتراضية من ٤٦٧ شركة مثل مايكروسوفت (Microsoft) وفيريزون (Verizon).

الجدول (٦-١): أسوأ ٢٥ كلمة مرور، ٢٠١١

password	12345	letmein	michael	2000
123456	dragon	monkey	shadow	jordan
12345678	rosey	696969	master	superman
1234	baseball	abc123	jennifer	harley
qwerty	football	mustang	111111	1234567

عند اكتمال تثبيت خادم تعليمات الاستعلام البُنيوية (Microsoft SQL Server 2000) فإن حساب مسؤول قاعدة البيانات « sa» يظل دون كلمة مرور.

وفي شـهر يوليو من عام ٢٠١٢ اكتشف أحد مزودي خدمة الإنترنت الرئيسين في هولندا أن حسـابات العملاء معرضة للاختراق بسـبب بيانات الاعتـماد الافتراضية؛ إذ جرى إعداد اسم المستخدم ليتكون من الرمز البريدي بالإضافة إلى عنوان الشارع، في حين تم ضبط كلمة المرور الأولية لتكون «welkom01». وعندما جرى القيام بالفحص الأمني على الحسـابات تـم اكتشـاف أن ١٤٠ ألف عميل لم يكلفوا أنفسـهم عناء تغيير كلـمات المرور الافتراضية الأولية.

والاختلاف الطفيف في الموضوع هو نقطة الوصول اللاسلكي (Wireless Access Point) والتي قد يكون لديك مثلها في المنزل. فمن أجل الربط بجهاز التوجيه المنزلي (home router) والوصول إلى الشـبكة اللاسلكية تحتاج إلى اسم الشـبكة والذي يتم بثه واكتشافه من قبل جهاز الحاسـب الآلي، كما تحتاج إلى كلمة مرور الموجـه. وهناك نوعان من كلمات المرور

الشائعة لنقاط الوصول اللاسلكي (WAPs) والتي يتم توزيعها من قبل مزود خدمة الإنترنت: أمــا أن تكون عنوان جهاز التوجيه المادي (MAC address)، أو قيمة ســت عشرية أخرى (hexadecimal value). ويمكن العثور بســهولة على كلمة المرور التي تكون مكتوبة على الجانب السفلي من نقاط الوصول اللاسلكي (WAPs). وكل ما يحتاج إليه قراصنة الحاسب وصول سريع إلى الشــبكة الخاصة بك خلال اجتماع أو احتفال وبعد ذلك ســيكون لديهم إمكانية الوصول الفوري للشبكة.

تحرير أجهزة الهاتف المحمول «الآيفون» (Jailbreaking iPhones)

في عام ٢٠١٠ بدأت الجامعات ملاحظة موجة جديدة لمسح منافذ الشبكة تستهدف منفذ رقم ٢٢ وهو المنفذ المخصص للوحة المراقبة المشفرة المتعلقة بحارس القشرة الآمنة (Security Shell Daemon(SSHd . وعند تعقب بروتوكول الإنترنت، تم اكتشاف أن ذلك على صلة بتحرير أجهزة الهاتف المحمول (iPhones).

ويشير مصطلح (jailbroken) إلى حقيقة أن نظام تشغيل الهاتف المحمول (iPhone lOS) يتم استبداله بنظام تشغيل آخر من قبل المستخدم. إن تحرير أجهزة الآيفون عملية سهلة يتم من خلالها إزالة بعض القيود التي تفرضها شركة أبل على مطوري التطبيق. لكن اتضح أن عملية التحرير تُضيف خادم القشرة الآمنة (Security Shell Server) لجهاز الآيفون بحساب افتراضي بمسمى «جذر» وكلمة مرور افتراضية هي «alpine». إن مسحاً سريعاً للشبكة وللمستخدمين يقود لأجهزة الهاتف المحمول (iPhones) المحررة بكلمات مرور افتراضية مما يؤدي إلى أن يكون التصرف في تلك الأجهزة «مملوكاً» لقراصنة الحاسب.

هجمات تجاوز سعة المخزن المؤقت (Buffer overflow attacks):

دعنا نبدأ هذه الجزئية بمثال. تجاوز ســعة المخــزن المؤقت مثل وضع جالون من الماء في إناء ســعته كوب واحد فقط. في نهاية المطاف سيطفح الماء وسيستخدم الأماكن الأخرى التــي يُفترض ألا يذهب إليها. وعادة يضيع الفائض ولا يتم الاســتفادة منه. ولكن في عالم الكمبيوتر الفائض المشكّل بدقة يمكن أن يسفر عن مفاتيح العالم.

في عــالم الحوســبة، يحدث تجاوز ســعة المخزن المؤقت عندما تكون أبعــاد البرنامج أو الإناء غير محددة بشكل جيد. والمحتوى الذي كان من المفترض أن يناسب الذاكرة، يطفح و«يتجاوز» أجزاء أخرى من ذاكرة الحاســب الآلي. وإذا كان محتوى الفائض مصمماً بشكل جيــد فإنه يمكن «خداع» جهاز الحاســب الآلي وإقناعه بــأن الفائض هو في الواقع جزء من البرنامج ويحتاج إلى تشغيل.

رمز الاختراق (Hello World) في لعبة سوني بلاي ستيشن الجديدة (PS Vita)

تُعد ألعاب سوني بلاي ستيشن (Sony's PSP) المفضلة بين قراصنة الحاسب الآلي وذلك لسهولة اختراقها. ويمكن تغيير وحدة التحكم المحمولة للعب بألعاب وبرامج تقليدية والمعروفة باسم (homebrews). ومع الكشف عن لعبة بلاي ستيشن الجديدة والتي تسمى (PS Vita)، تأمل شركة سوني أن أيام الاختراق قد ولت دون رجعة. وللأسف كانت شركة سوني مخطئة.

تمكن قرصان حاسب ياباني يحمل الاسم المستعار (Wololo) من نشر أول رمز اختراق (Hello World) على لعبة بلاي ستيشن الجديدة (PS Vita). وباستخدام تجاوز سعة المخزن المؤقت، تمكن قرصان الحاسب من إيجاد طريقه إلى اللعبة الجديدة. ومع العديد من الاختراقات لألعاب سوني بلاي ستيشن التي لم تنشر لمجتمع الألعاب ولا لقراصنة الحاسب الآلي، فإن الألعاب والبرمجيات ستستمر في المدى القصير على البلاي ستيشن الجديدة (PS Vita).

وتســتخدم دودة الرمز الأحمر (Code Red worm) تجاوز ســعة المخزن المؤقت من خلال الاتصال بثغرة في خادم (Microsoft IIS Server) ومن ثم إرساله لسلسلة كبيرة من حروف (N) (حرف-N-كبير). وفي نهاية السلسلة تقوم الدودة بإرسال مقطع من تعليمات برمجيات ليتم تنفيذه من قبل خادم الشبكة. بسيطة وفعالة!

حماية المُجمِع (Compiler protection) ضد المشكلات المعروفة لتجاوز سعة المخزن المؤقت

تقوم البرامج المُجمِعة الجديدة بتحذير المستخدمين أثناء قيامها بتجميع البرامج التي تحتوي على وظائف خطيرة ومعرضة لتجاوز سعة المخزون المؤقت:

```
user@server -/user $ gcc simple.c -0 simple
/tmp/ccECXQAX.o:  In function 'main':
simple.c:  (.text+0x17):  warning:  the 'gets' function is dangerous and should not be used.
```

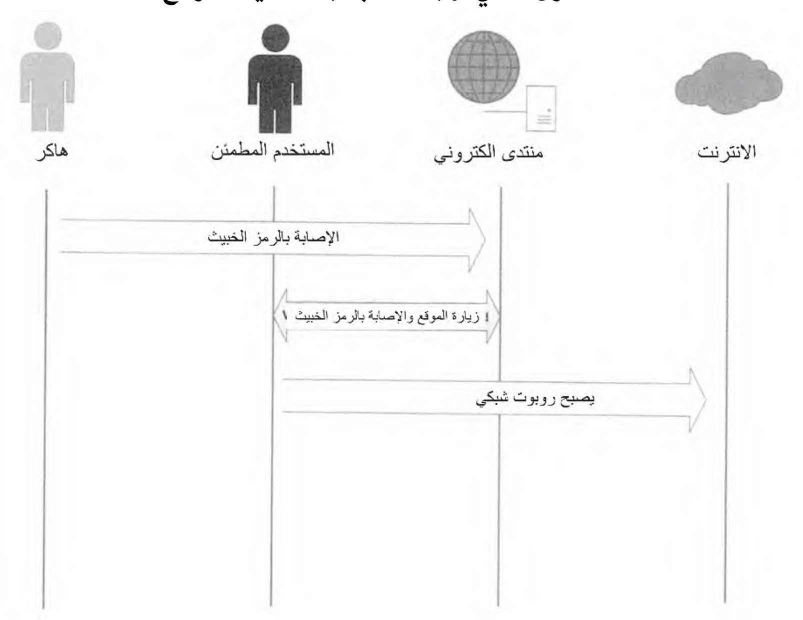
هجمات البرمجة النصية للمواقع المشتركة (Cross-site scripting (XSS) attacks):

وهذه الهجمات هي الأكثر شــيوعاً على شبكة الإنترنت. وتحدث هذه الهجمات عندما يســمح الموقع الإلكتروني لمســتخدم مُخرِب بإدخال معلومات ذات محتوى مُضِر. ويكون المحتوى عادة رمز جافا ســكربت (javascript code) يتم تشغيله في جهاز العَميل عندما يقوم بزيارة الموقع. والأهداف الشائعة لهذه الهجمات هي المنتديات على شبكة الإنترنت. وعــادة لا تتحقق برمجيات تشــغيل هــذه المواقع من مدخلات المســتخدم مما يســمح للمســتخدمين بإدخال رمز إتــش تي إم إل (html code) أو رمز جافا (javascript code) ثم يتم نشر الرمز في المنتدى حتى يقوم المستخدمون الآخرون بتشغيله (الشكل ٦-١١).

ووفقــاً لشركــة (Accunetix)[١٦]، وهي شركة متخصصــة في أدوات تقييم الثغرات على شــبكة الإنترنت، فإن المواقع الإلكترونية المُســتغلَة من قبل هجمات (XSS) تُستخدم عادة للقيام بالأنشطة الخبيثة التالية:

- انتحال الشخصية.
- الوصول إلى معلومات حساسة أو معلومات مقيدة.
- الحصول على وصول مجاني لمحتوى غير مجاني.
- التجسس على عادات التصفح لمستخدمي الإنترنت.
- تغيير وظائف المتصفح.
- التشهير العام بفرد أو بمنظمة.
- تشويه تطبيقات الإنترنت.
- هجمات رفض الخدمة.

شكل (٦-١١): المستوى العالي لهجمات البرمجة النصية للمواقع المشتركة



(16)http://www.acunetix.com/websitesecurity/cross-site-scripting/

وفيما يلي مثال مبسط لهجوم (XSS). ويبدأ المثال بالرمز الموضح أدناه وذلك للوصول لصفحة الإنترنت بحيث تحصل هذه الصفحة على رمز للمتغير (وعادة ما يكون ذلك المتغير اسماً) من عنوان الموقع (URL). وبعد ذلك يتم عرض رسالة ترحيبية على الشاشة.

```
php?>
;(‘name = $_GET[‘name$
;«<echo «My name is $name<br
/>echo «<a href=”http://xssattackexamples.com/”>Click to Download
;» >a
>?
```

ويمكن لقراصنة الحاسب أن يقوموا بصياغة عنوان الموقع (URL) إلى العنوان التالي:

```
index.php?name=guest<script>alert(‘owned’}</script>
```

ويعد هذا النوع من هجمات الـ (XSS) غير مستمر، وأنه إلى حد بعيد النوع الأكثر شيوعاً من الهجوم. ويحدث ذلك عندما تقوم البرامج النصية من جانب الخادم باستخدام البيانات المقدمة من قبل العملاء لإنشاء صفحة من النتائج لهذا المستخدم دون التحقق من صحة الطلب[١٧].

هجمات حقن تعليمات الاستعلام البُنيوية (SQL injection attack):

هجمات حقن تعليمات الاستعلام البُنيوية هي تقنية تستخدم لاستغلال كيفية تواصل صفحات الإنترنت مع قواعد البيانات الخلفية. ويمكن للمهاجم إصدار أوامر إلى قاعدة بيانات (على شكل عبارات SQL صممت خصيصاً لهذا الغرض) باستخدام حقول الإدخال في الموقع الإلكتروني[١٨]. وكما ترى أن هجمات حقن تعليمات الاستعلام البُنيوية مشابهة إلى حد كبير لهجمات البرمجة النصية للمواقع المشتركة (XSS). الفرق الأساسي هو أن هجمات (XSS) تُنفذ في الواجهة الأمامية للموقع الإلكتروني في حين أن هجمات حقن تعليمات الاستعلام البُنيوية تُنفذ في الخادم. والمشكلة في كلا الحالتين أنه لا يتم التحقق من مدخلات المستخدم بالشكل الصحيح.

---

(١٧) بإمكانك مشاهدة مثال لهجمات الـ (XSS) غير المستمرة على موقع (http://www.insecurelabs.org).

قام أصحاب هذا الموقع بتصميمه خصيصاً ليكون عرضة لهجمات الـ (XSS). اختر واحداً من بنود الجدول وألصق النص البرمجي الموجود أعلاه. وإذا كان الجافا سكريبت مفعلاً في متصفح الشبكة الخاص بك سترى الرسالة «المملوكة» تظهر على سطح الشاشة.

(18) Verizon’s Data Breach Investigations Report (n.d.). Retrieved from http://www.slideshare.net/cloudrunnertom/verizon-dbir

ومثال على ذلك، دعنا نفترض أن موقعاً إلكترونياً يسمح لك بإدخال اسم العائلة في مربع نص، وعند الضغط على إرسال، يقوم الموقع بعرض الاسم الأول مع رقم الهاتف. الاستعلام الذي يُرسله خادم الشبكة إلى قاعدة البيانات الخلفية قد يبدو مثل الاستعلام التالي:

```
SELECT fname, phone FROM contacts WHERE lname = 'doe'
```

لكن ماذا لو أدخلنا النص التالي في مربع النص:

```
doe' OR '١=١';
```

ولأن شرط «١=١» دائماً صحيح فإن قاعدة البيانات ستقوم بعرض كافة محتوياتها. ولكن الأمر قد يزداد سوءاً.

```
doe' exec master.dbo.xp_cmdshell 'iisreset/Stop'
```

إذا كان خادم قاعدة البيانات يسمح للقشرة بالهروب (يمكن تنفيذ الأوامر خارج بيئة قاعدة البيانات، على نظام التشغيل نفسه)، فإن المدخلات أعلاه ستقوم بإيقاف خادم الشبكة (IIS web server) على الجهاز.

في عام ٢٠١٢ قامت مجموعة القراصنة المعروفة باسم مجموعة (المجهول) «Anonymous» باستخدام حقن تعليمات الاستعلام البُنيوية ضد واجهات الشبكة غير المحصنة وذلك للكشف عن المعلومات المخزنة في خوادم قواعد البيانات لـ ٥٠ جامعة حول العالم، متضمناً ذلك جامعات برينستون (Princeton)، جون هوبكنز (John Hopkins)، وروتجرز (Rutgers)[١٩].

إساءة الاستخدام:

إساءة الاستخدام يتضمن الاستخدام غير المصرح به للأصول. وفي معظم الحالات فإن إساءة الاستخدام تأتي نتيجة لغياب مبدأ الأمن العام المعروف باسم «الحاجة للمعرفة». واستناداً إلى مبدأ الحاجة للمعرفة فإن الفرد لا يكون لديه حق الوصول إلى الأصول إلا إذا كان يحتاج إلى ذلك لأداء وظيفته. وهذا المبدأ ينطبق بشكل مستقل عن الوظيفة التي يشغلها الشخص في المنظمة.

(19) http://pastebin.com/AQWhu8Ek

إساءة استخدام الامتيازات:

يحدث إســاءة اســتخدام الامتيازات عندما يســتخدم الموظف منصبه و/أو الوصول إلى الأصول بطريقة غير سليمة مما يتسبب في الضرر للأصول و/أو المنظمة.

وكشــخص متخصص في تقنية المعلومات، أول ما يتبادر إلى الذهن هو إســاءة استخدام مســؤولي النظم لامتيازاتهم. لنأخذ على ســبيل المثال ستيفن بارنز (Steven Barnes) أحد متعهدي تقنية المعلومات. عمل ستيف لشركة (Blue Falcon Networks) والمعروفة الآن باســم (Akimbo Systems). وفي عام ٢٠٠٨ صدر حكم مــن محكمة في ولاية كاليفورنيا على ستيفن بدفع ٥٤ ألف دولار كتعويضات لشركة (Akimbo Systems)، كما حُكم عليه بقضاء ســنة واحدة ويوم واحد في السجن. والسبب أن ستيفن استخدم صلاحياته للدخول على خادم البريد الإلكتروني للشركة (Exchange email server) لإزالة القيود التي وضعت لحماية الخادم من مُرســلي البريد المزعج ومن ثم جرى استخدام الخادم كبروكسي للرسائل غــير المرغوب فيها. وكانت النتيجة مشــابهة لهجمات الحرمان مــن الخدمة حيث تعطل نظام البريد الإلكتروني لشركة (Akimbo Systems) وذلك عندما وجد مُراسلو البريد المزعج المنافذ مفتوحة. ووفقاً لســتيفن فإنه فتح المنافــذ انتقاماً من زملاء العمل في شركة (Blue Falcon Networks) والمعروفة الآن باســم (Akimbo Systems)، والذين جاؤوا إلى منزله وأخذوا أجهزة الحاسب الآلي الخاصة به بالقوة وذلك في عام ٢٠٠٣ [٢٠].

الاحتيال والاختلاس:

يُعــد قانــون الاحتيال وإســاءة الاســتخدام والوصــول المزيف لأجهزة الحاســب الآلي (Counterfeit Access Device and Computer Fraud and Abuse Act)، والــذي أقــره الكونغرس في عــام ١٩٨٤، أول محاولة من قبل الحكومة الاتحادية للتعامل مع قضية احتيال في مجال تقنية المعلومات. كما يجرم القانون استخدام أجهزة الحاسب الآلي لإلحاق الضرر بأنظمة الحاسب الآلي، متضمناً ذلك الأجهزة والبرمجيات الخاصة بها. وهذا القانون موجه في المقام الأول نحو قراصنة الحاسب الآلي. ومنذ ذلك الحين تم استخدام هذا القانون

(20) http://gawker.com/5076432/angry-angry-it-guy-goes-to-jail

لمقاضــاة الموظفين الذين يســتغلون مناصبهم للوصول إلى أصــول المنظمة بهدف الاحتيال واختلاس الأموال من المنظمات وعملائها.

إن حالات الاحتيال والاختلاس باستخدام موارد تقنية المعلومات كثيرة، وخصوصاً عندما يجد الأفراد أنفسهم في ضائقة مالية. وقد أدى ذلك إلى قيام الشركات بالتحقق من الرصيد الدائن للموظفين الذين لديهم امتياز الوصول إلى أصول قد ترتبط بها عمليات احتيال.

وفي شهر أغسطس من عام ٢٠١٢ بدأت امرأة من نوكسفيل (Knoxville) بقضاء خمس ســنوات تحت المراقبة بعد اعترافها بارتكاب عملية احتيال باســتخدام أجهزة حاســب آلي وذلك أثناء عملها مديرة عمليات التجزئة في مصرف ســن ترســت (SunTrust Bank)[٢١]. وكانــت وظيفتها التأكد من أن الفروع في منطقتها تمتثل لممارســات الأمــن الداخلي، وفقاً لأعضاء النيابة العامة. وكان لديها إمكانية الوصول إلى الســجلات المالية لعملاء سن ترست من خلال جهاز الحاســب الآلي المخصص لعملها، وفقاً للمدعي العام. وفيما يلي أمثلة أكثر على الاحتيال باستخدام أجهزة الحاسب الآلي:

- إرســال خدع عبر البريد الإلكتروني بهدف تخويف النــاس (البرمجيات المُثيرة للقلق، وبرمجيات الفدية).
- اســتخدام جهاز الحاسب الآلي لشــخص آخر بطريقة غير شرعية أو «التظاهر» بأنه شخص آخر على الإنترنت.
- استخدام أي نوع من البرمجيات الخبيثة أو رسائل البريد الإلكتروني لجمع المعلومات من منظمة أو شركة بقصد استخدامها لتحقيق مكاسب مالية.
- استخدام أجهزة الحاسب الآلي لإغواء القاصرين في تحالفات جنسية.
- انتهــاك قوانــين حقوق التأليف والنــشر عن طريق تحميل وتبــادل مواد محفوظة الحقوق دون إذن صاحبها.
- استخدام أجهزة الحاسب الآلي لتغيير المعلومات، مثل الدرجات، وتقارير العمل، وغيرها.

---

(٢١) الحكم على موظفة سابقة في بنك سنترس في قضية احتيال باستخدام أجهزة الحاسب الآلي، تم استعادتها من الموقع http://www.knoxnews.com/news/local/former-suntrust-bank-employee-sentenced-in-computer-fraud-case-ep-361004043-357098531.html

استخدام البرمجيات غير المعتمدة:

قد يصبح الموظفون وسـطاء تهديد عندما يقومون بعمل لا يتفق مع سياسـة المنظمة كتثبيـت تطبيقات برمجية على أجهزة الحاسـب الآلي. البرامج المثبتة في أجهزة الحاسـب المكتبية أو الهواتف الذكية قد توفر لقراصنة الحاسـب وسـيلة للوصول إلى الأصول المقيدة للمنظمة.

ويُعد السـماح للمسـتخدمين بتثبيت البرمجيات على الحواسب المكتبية قضية إشكالية خصوصاً بالنسبة للجامعات. وبشكل تلقائي يجب أن تكون الجامعات مفتوحة وغير مقيدة لأنها المكان الذي يجتمع فيه حب الاسـتطلاع والبحوث لتشـجيع الإبداع. من جهة أخرى يمكن أن الانفتاح نفسـه يُعرّض البيانات البحثية وغيرها من الأصول المعلوماتية إلى وسطاء تهديد مما يؤدي إلى عواقب وخيمة على الوحدة الإدارية والأفراد.

وخير مثال على القضايا المرتبطة بتثبيت البرمجيات هو برنامج (Bonzi Buddy) والذي ظهر في أواخر التسـعينيات، كان الغوريلا الأرجواني (Bonzi) اللطيف والرائع، وكان مُفضلاً لدى كثير من المستخدمين في الحرم الجامعي، وكان يتجول على سطح مكتب جهاز الحاسب الآلي وكان يُسلي المستخدمين. ولسوء الحظ كان أيضاً يجمع معلومات عن عادات التصفح الخاصة بالمسـتخدم، ومحلات التسوق المفضلة للمسـتخدم (برنامج تجسس-spyware)، ومـن ثم يعرض الإعلانات ذات الصلة على الشاشـة (برنامج إعلانـات تطفلي –adware). وأخيراً فإنه يسـتخدم الكثير من طاقة وحدة المعالجة المركزية (CPU) مما يؤدي إلى بطء شديد في جميع التطبيقات الأخرى الشكل (٦-١٢).

وبسـبب انفتاح الجامعات على العالم الخارجي فإنها لا تملك سياسة حظر المستخدمين من تثبيت البرمجيات على أجهزة الحاسـب الآلي، ولكن العديد من المنظمات الأخرى تقوم بذلك. ففي شـهر أغسـطس من عام ٢٠١٢ قـررت المحكمة الجزئيـة الأمريكية للمنطقة الغربيـة مـن ولاية أوكلاهوما أن الموظـف الذي يقوم بتحميل برمجيـات من الإنترنت في انتهاك لسياسـة المنظمة قد يكون مسـؤولاً بموجب قانـون (CFAA) عن قيام البرمجيات المُحمَلة بالحصول على وثائق المنظمة السرية. ففي القضية التي كانت بين شركة (Musket Corp) وشركـة (Star Fuel of Oklahoma LLC)، رأت المحكمـة أن أي شـخص مخول

لاســتخدام جهاز الحاســب الآلي لأغراض معينــة ولكنه يتعدى تلك الحــدود، فإنه يُعد قد «تجاوز الوصول المسموح» وفقاً لقانون (CFAA).

يأتي تغيير التهديد (threat shifting) استجابة من قراصنة الحاسب للتحكم في الوضع، وذلك بتغيير خصائص الأهداف/ المستهدفين من أجل تجنب و/أو التغلب على إجراءات الوقاية المضادة[٢٢].

الشكل (٦-١٢): برنامج (Bonzi Buddy)



الهندسة الاجتماعية:

الهجمات الاجتماعية تشمل محادثات أو حوار مع مستخدمين بهدف إقناعهم أن يفعلوا شيئاً لا يقومون عادة بفعله. وفي ظروف معينة حتى مستخدمو الحاسب الآلي الأذكياء قد يكونون عرضة لهجمات الهندسة الاجتماعية.

التحجج الاحتيالي (Pretexting):

وهي التقنية التي يستخدم فيها المهاجم سيناريو وهمي للتأثير في شخص ما لإنجاز عمل ما أو بهدف إفشاء معلومات. ويعرف (التحجج الاحتيالي) خارج المنطقة الفنية باسم (لعبة الخدع-con game) أو (الاحتيال-scam).

---

(٢٢) دليل تقييم إجراء المخاطر، #2fishygirl on Scribd (n.d.). Retrieved from https://www.scribd.com/document/65740364/Guide-for-Conducting-Risk-Assessments

وأحد أنــواع التحجج الاحتيالي هو الانتحال (phishing) والذي يســتخدم فيه المهاجم البريد الإلكتروني في محاولة لجعل متلقي الرســالة الإلكترونية يفصح عن بعض المعلومات. ويمكن أن تكون رســائل الانتحال الإلكترونية مقنعة وجميلة وجذابة بشكل كبير، كما يمكن أن يأخذ المرســل دور شــخصية ذات سلطة، أو يأخذ دور شخص يعرفه المستخدم. ويقترن الانتحال عادة برســائل البريد الإلكتروني غــير المرغوب فيها (spamming) وهي التي يقوم فيها المهاجم بإرســال آلاف وآلاف من الرســائل الإلكترونية على أمل إقناع نسبة صغيرة من المتلقين بفتح ملف مصاب ببرمجيات خبيثة، أو الرد برقم الحساب أو كلمة المرور.

التصيد الانتحالي في صحيفة فاينتشال تايمز

في التاسع والعشرين من شهر مايو من عام ٢٠١٣ أعلنت صحيفة فاينتشال تايمز أن هجوماً انتحالياً ناجحاً قد اصطاد على حين غرة صحفيين ذوي اطلاع واسع في الصحفية الموقرة حيث كانت الرسائل الإلكترونية موجهة ومصممة خصيصاً لصحفية الفاينتشال تايمز. وتمكن قراصنة يطلقون على أنفسهم اسم الجيش السوري الإلكتروني (Syrian Electronic Army)، ربما بعد الأحداث الجارية في سوريا في ذلك الوقت، من الوصول إلى حسابات البريد الإلكتروني لكثير من الصحفيين المخضرمين. ولقراءة المزيد من التفاصيل بإمكانك الرجوع إلى رابط الصحيفة الموجود أدناه.

والميزة المثيرة للاهتمام في هذا التقرير هو الإشارة إلى أن العديد من المنظمات تعترف بكل أريحية أنها وقعت ضحية لتلك الهجمات، وتوضح كيف يمكن للمنظمات الأخرى، بما في ذلك منافسيهم، أن ينقذوا أنفسهم من عار الوقوع ضحايا لهجمات مماثلة. وهذا تطور كبير عما كان يحدث قبل بضع سنوات عندما كان من النادر أن تعترف المنظمات بمثل تلك الهجمات علناً.

المرجع:

Betts, A. «A sobering day,» Financial Times labs, http://Iabs.ft.com/201305//a-sobering-day/ (accessed 071612013/)

ومــع توجه الاتصالات الهاتفية لما يعرف بالتواصل الصوتي عبر شــبكة الإنترنت (Voice Over IP) أو اختصــاراً (VOIP)، ظهــرت طريقــة جديــدة لهجمات التحجــج الاحتيالي (pretexting). وتعــرف هذه الطريقة بـ (Spam over Internet Protocol) أو اختصاراً (SPIT) وهي عبارة عن مجموعة من المكالمات الهاتفية المســجلة مسبقاً باستخدام شبكة مخترقــة من شــبكات (VOIP). ومن خلال هذه الطريقة يتم توجيه الشــخص الذي يرد على المكالمة «بالبقاء على الخط» أو الإجابة عن أســئلة والتي يتم تسجيلها ونقلها لقراصنة

الحاسـب. وبعكس تسـليم البريد الإلكتروني حيث يوجد عنـاصر للتحكم لإيقاف معظم الرسـائل غير المرغوب فيها والتي تصل للمسـتخدم، لا يوجد طريقـة للتحكم في المكالمات الهاتفيـة التي تصل إلى هاتف شـخص ما. وبينما كان لدى بعـض شركات الهاتف «قوائم سـوداء» متاحة للعملاء (مقابل رسـوم رمزية)، إلا أن الوضع يكون خارج السـيطرة عندما يتغير مصدر المكالمات بشكل دوري.

نشاط التهديد المادي (Physical):

وهذا يتضمن الجانب المادي أو الجانب الملموس للأصل. ولسوء الحظ فإن العديد من المنظمات لا تأخذ نشاط التهديد المادي بعين الاعتبار بما فيه الكفاية لتبرير تكاليف الحماية ضد تلك الأنشطة التهديدية.

الدخول غير المرخص:

وهـذا تهديد شـائع حيث تتطلب العديد من المنظمات وجـود بعض المناطق المحمية بآلية الدخول بالبطاقة. لكن وفي محاولة ليصبح الموظفون مهذبين ووديين، يقوم الموظفون بإبقاء الباب مفتوحاً عند رؤيتهم لشـخص ما يركض لاسـتغلال هذه الفرصة لدخول المبنى دون البحث عن بطاقته الخاصة بالدخول. وفي كثير من الأحيان لا يقوم الموظفون بتحدي الأفراد الآخرين خصوصاً إذا كانوا يعاملون أنفسـهم بثقة وإيمان انطلاقاً من مبدأ «يُفترض أن أتجول هنا بدون بطاقتي الخاصة بالدخول».

نعيش في عصر تحول فيه الإرهاب من وسـيط تهديد غير معروف نسـبياً إلى مشـكلة كـبرى، لذا فإن التحكم في الدخول غـير المصرح به إلى المناطق والأنظمـة المتعلقة بالبنية التحتيـة مثل المطارات ومحطات توليد الطاقة وحتى محطات الكهرباء التي تخدم منطقة محـدودة أصبح قضية حرجة. وفي حين أن الأسـوار وضوابط الوصول الأخرى كانت مبدئياً تهـدف في المقام الأول لمنع الناس مـن الوصول ولإصابتهم بصعقـة كهربائية، لكن ما يثير القلق الآن هو أن الوصول غير المصرح به سـيؤدي إلى نقص حاد في خدمات البنية التحتية الحرجـة. والمنظـمات الآن تراجع المبادئ التوجيهية والمعايـير لحماية الأصول، مثل معهد مهندسي الكهرباء والإلكترونيات (Institute of Electrical and Electronics Engineers)

ومعاييرهــم الخاصة بالأمن المادي لمحطات التوليــد الكهربائية (Standard for Physical Security of Electrical Power Stations)(٢٣)، وذلــك للتركيــز عــلى وســطاء التهديد الجديدة وتلك التي تم تجاهلها سابقاً.

مكتبة بارنز ونوبلز (Barnes and Nobles)

في شهر أكتوبر من عام ٢٠١٢ تعرض عملاء المكتبة العملاقة بارنز ونوبلز (Barnes and Nobles) لسرقة أرقام بطاقات الصرف البنكية وأرقامها السرية، وذلك عندما تم العبث بمنصات الدخول في ٦٣ محلاً (وهذا نشاط تهديد مادي آخر) وذلك لتسجيل المعلومات التي استُخدمت للدفع من جميع العملاء. وتم اكتشاف المنصات التي تم العبث بها في مواقع متعددة في جميع أنحاء الولايات المتحدة الأمريكية، وكل المؤشرات تدل على وجود دخول غير مصرح به إلى نقاط إدخال البيانات تلك.

السرقة:

عند التجول في الحرم الجامعي أو مكتبة الجامعة أو منطقة دراسية أخرى، ستلاحظ أنه من الســهل أن تأخذ جهاز الحاسب الآلي المحمول لشخص ما عندما يخرج بسرعة للذهاب إلى دورة المياه. ســيكون لديك متســع من الوقت لإغلاق غطاء الحاسب المحمول، وتفصل الكهرباء من المقبس، وتنطلق بالجهاز الجديد.

سرقة (AvMed)

في عام ٢٠٠٩ تمت سرقة جهازين حاسب آلي تحتوي على ١,٢ مليون سجل لعملاء شركة طبية تُدعى (AvMed Health Plans) من مكتب مدينة غاينيسفيل في ولاية فلوريدا. استغرقت الشركة ٣ أشهر لفهم مدى الاختراق، ولإشعار العملاء المتضررين. وتحتوي السجلات المحفوظة في أجهزة الحاسب الآلي المسروقة على أسماء أعضاء الشركة، وعناوين المنزل، وأرقام الهاتف، وأرقام الضمان الاجتماعي، وغيرها من البيانات الحساسة للغاية مثل التاريخ الطبي، ومعلومات التشخيص، والإجراءات الطبية، ومعلومات الوصفات الطبية. ورُفعت دعوى قضائية في عام ٢٠١٠ نيابة عن العملاء.

الأخطاء (Error):

هذه الفئة من أنشــطة الوســطاء تشــمل كل عمل غير صحيح وغير مقصود. وتشمل الإهــمال، والحوادث، والعثرات، وأعطال الأجهزة والبرمجيات، وغيرها. والأخطاء لا تشــمل الأشياء التي تُركت دون إتمامها، أو الأشياء التي تم إتمامها بشكل غير صحيح ولكن عمداً.

(23) http://standards.ieee.org/develop/project/1402.html

أخطاء إدخال البيانات (Data entry errors):

أخطــاء ادخال البيانات تأتي على نوعين: الحــذف والزيادة. ومع وجود أخطاء الحذف لا يتم إدخال القيمة بطريقة مناسبة. أما أخطاء الزيادة فتؤثر في سلامة إدخال البيانات.

وللأســف فإن أخطاء إدخال البيانات شائعة لكنها خطيرة خاصة في مجال الصحة. وتم وضع الســجلات الصحية الإلكترونية للعمل بها في المستشــفيات ومكاتب الأطباء في جميع أنحــاء البلاد بهدف تســهيل تبادل البيانات بين الجهات الطبيــة وغيرها من نقاط الرعاية. لكن تبادل البيانات بهذه الطريقة من شــأنه أن يشارك أي خطأ في إدخال البيانات نفسها. وفي حين أن التكنولوجيا نفسها قد تكون مهمة، إلا أن كلاً من التدريب المناسب، واختبارات قابلية الاستخدام ضروريان لعمل هذه الأنظمة بالشكل الصحيح.

أخطاء التهيئة (Misconfiguration):

يجب على مســؤولي النظــام توخي الحذر عند تعاملهم مع الخــوادم التي تحتوي على معلومات شخصية. وللأسف فإن تحديث البرمجيات والأجهزة تتم عادة تحت ضغط هائل لإعادة توافر النظام بأسرع ما يمكن وذلك يؤثر في تكامل النظام وسلامته.

ويبدو أن حوادث أخطاء التهيئة الأكثر شيوعاً تكون ذات علاقة بتلك التحديثات. ففي عام ٢٠١٢ وفي جامعة نورث كارولينا في مدينة شــارلوت (Charlotte) أصبحت المعلومات الشــخصية لأكثر من ٣٥٠ ألف شخص مكشوفة بسبب فشل المسؤولين في ترحيل إعدادات الأمان بشــكل صحيح من الخادم القديم الذي توقف عن العمل للانتقال إلى خادم جديد. والشيء نفسه حدث مع كلية نورث ويست (Northwest College) في ولاية فلوريدا بعد هذه الحادثة ببضعة أشهر.

البيئة (Environment):

أنشطة التهديد التي تندرج تحت تصنيف البيئة تشمل ما يلي:

- الكوارث الطبيعية مثل الأعاصير، والعواصف، والفيضانات.
- فشــل الضوابط البيئية المخصصة لدعم أصول تقنيــة المعلومات، مثل انقطاع التيار الكهربائي، وتسرب المياه، وتعطل تكييف الهواء، وغيرها.

وسطاء الكوارث الطبيعية

قد يتبادر سؤال إلى الذهن: من أو ما هو وسيط التهديد للكوارث الطبيعية؟ يعتمد هؤلاء الوسطاء على الوجود الجغرافي للمنطقة التي تقع فيها أصول المنظمة. على سبيل المثال، يجب أن تكون المنظمات التي تقع في وسط غرب الولايات المتحدة قادرة على التعامل مع العواصف. وتمثل الأعاصير مصدر قلق على سواحل المحيط الهادئ والمحيط الأطلسي. ويجب أن تكون المنظمات التي تقع على الساحل الغربي حذرة أيضاً من الزلازل.

تعطل تكييف الهواء:

شركة (Level3) هي شركة اتصالات ضخمة متعددة الجنسيات مقرها في كولورادو. وتعمل هذه الشركة على النقل الشبكي للبيانات والصوت وتوصيل المحتوى لمعظم شركات الاتصالات في الولايات المتحدة والخارج.

في عام ٢٠١١ تعرضت الشركة لتعطل تكييف الهواء في أحد مراكز بياناتها والذي يقع في فرنسا. ولأن الاحتفاظ بمركز البيانات يكون مكلفاً فإن الشركة تسعى لأن تملأ مركز البيانات بأكبر عدد ممكن من الخوادم لتقليل تكاليف الدعم. ونتيجة لذلك فإن حفظ الهواء البارد أمر ضروري. وبعد ساعات قليلة، وصلت درجة حرارة محيط غرفة الخادم إلى ١٣١ درجة فهرنهايت. وعندما وصلت درجة الحرارة إلى تلك النقطة، بدأت اللوحة الإلكترونية الأساسية (motherboard) والدوائر المتكاملة بالتعطل. وقد تعود الأقراص الصلبة للعمل إذا عادت درجة الحرارة إلى وضعها الطبيعي لكن المشكلات المتعلقة بالرؤوس واللوحات الجافة تبقى كامنة لعدة أشهر قبل أن تعاود الظهور في أي فحص مُحتمل لهذه الأجهزة.

وسبب المشكلة في هذه القضية واضح. تعتمد أنظمة تكييف الهواء على إمدادات مياه مبردة حتى تعمل. وفي وقت سابق من ذلك اليوم تعرض خط إمدادات المياه المبردة لنظام تكييف مركز البيانات الفرنسي للانفجار. وبدون مصدر بديل للمياه المبردة لا يمكن لنظام التكييف أن يعمل وقد تم إيقافه.

الأعاصير (Hurricanes):

نحن في شركة في الطابقين العاشر والحادي عشر من ناطحة سحاب على طريق (Poydras Ave) وبالقرب من شارع (St. Charles). لدينا مولدات كهربائية وأطنان من الطعام

والمياه. ومجموعنا خمســة أشخاص. لســت متأكداً كيف سيتأثر الاتصال بالإنترنت. لدي كاميرا ومسدسي. وتصل سرعة الرياح إلى ١٧٥ والعاصفة إلى ٢١٥. الخطر الحقيقي ليس في الرياح بل في العاصفة التي تدفع بالرياح إلى المدنية من الخليج عبر البحيرة. وقد لا تتعافى المدينة مطلقاً. وبصراحة قد يكون هذا الأمر جسيماً[(٢٤)].

الاقتباس السابق تم نشره من قبل مايكل بارنيت (Michael Barnett) وهو قائد سابق في الجيش ومستشــار ســابق لشركــة (Intercosmos Media Group) وهي الشركة الأم لشركة اســتضافة المواقع الإلكترونية (zipa.com). وتم توظيف بارنيت أساساً بصفة مدير أزمات وذلك مع اقتراب عاصفة كاترينا. وظل مع صديقته في مركز البيانات لحماية الأصول ولحسن الحظ أنه خرج سالماً من العاصفة.

وأثبت إعصار كاترينا بأنه وحش تسبب في أضرار تقدر بعشرات الملايين من الدولارات. ومن موقعه في الطابق العاشر وثّق بارنيت الفوضى والنهب وصراعه للحفاظ على اســتمرار العمليات مع تضاؤل الموارد. وللأسف هذا لن يكون الإعصار الأخير. ففي كل عام، من شهر يونيو إلى شــهر سبتمبر، تســتعد المنظمات التي مقرها بالقرب من المناطق المعرضة للرياح والفيضانات المرتبطة عادة مع الأعاصير. وهذه واحدة من أكثر التهديدات المدمرة لواجهة مراكز البيانات والأصول التي تؤويها[(٢٥)].

الثغرات:

عرّفنا الثغــرات بأنها نقاط الضعف في نظم المعلومات والتي تعطي التهديدات الفرصة لاختراق الأصول. وغالباً يستخدم التعبيران: الثغرات والتهديدات، بالتبادل في هذه الصناعة خصوصاً من قبل الموردين. ومع ذلك فإنه من المهم التمييز بين هذين التعبيرين. وفي حد ذاتها فإن الثغرة لا تشكل خطراً على الأصول. وبالطريقة نفسها فإن التهديد لا يشكل خطراً ما لم يكن هناك ثغرة في النظام يمكن استغلالها من قبل التهديد.

(24) http://www.baselinemag.com/c/a/Business-Intelligence/Diary-of-Disaster-Riding-Out-Katrina-in-the-Data-Center

(25) يرجى الاطلاع على هذه المقالة للحصول على بعض الأمثلة الجيدة جدا من تصريحات التهديد: Adam L. Pineberg, «challenged hackers to investigate me and what they found is chilling», https://pando.com/2013/10/26/i-challenged-hackers-to-investigate-me-and-what-they-found-out-is-chilling/

ليس كل ثغرة تســبب تهديداً للشــبكة، ولا يجب تصحيح جميــع الثغرات على الفور. الثغرات التي يمكن اســتغلالها فقط هي التي تمثل تهديــداً على عمليات المنظمة والأصول المعلوماتية. ومن الشــائع للفرق الإدارية اســتلام تقارير عن الثغــرات مع طلبات لاتخاذ إجــراءات فورية للقضاء عليهــا. وأحد مصادر هذه الطلبات هو فريــق التدقيق الداخلي للمنظمة. والمصدر الشــائع الآخر لرسائل (أصلحه الآن لأن الصحافة أو الموردين يعتقدون بأهميته) هو الإدارة بما في ذلك العديد من مديري نظم المعلومات. لكن هل ينبغي النظر إلى جميع الثغرات بأنها حالات طارئة؟ وهل جميع الثغرات تســتحق التكاليف المالية من الميزانية الأمنية؟[٢٦]

اقتباس جانبي: «التهديد الفوري» (zero-day threat) هو التهديد الذي قام بتطويره وسيط التهديد قبل وجود حل للقضاء على الثغرة، وقبل نشر ذلك الحل للعامة.

ويستخدم وسطاء التهديد معرفتهم بالثغرات لإنتاج تهديدات جديدة ضد أحد الأصول. وبالنســبة للأصــول المعلوماتية فإن التعديل على رموز البرمجيــات لمعالجة الثغرات يُعرف بـــ «تصحيح الأمــان» (security patch). وأفــادت إدارة الأمن الداخــلي لقاعدة بيانات الثغرات الوطنية (Department of Homeland Security›s National Vulnerability Database)[٢٧] بوجود ٣٥٣٢ ثغرة في عام ٢٠١١ أي بمعدل ١٠ ثغرات جديدة تكتشف كل يوم. وهذا في الواقع يُعد تحسناً مقارنة بأرقام عام ٢٠٠٩ وعام ٢٠١٠ (الشكل ٦-١٣).

اختراق قاعدة بيانات الثغرات الوطنية
تم وضع قاعدة بيانات الثغرات الوطنية (NVD)، والتي تدار من قبل المعهد الوطني للمعايير والتقنية (NIST)، خارج الخدمة وذلك عندما لاحظ المشرفون نشاطاً مشبوهاً أدى إلى اكتشاف اثنين من البرامج الخبيثة على خوادم الشبكة الخاصة بها. ويُعتقد أن الخوادم اختُرقت لمدة شهرين على الأقل. وجرى الاختراق عن طريق الثغرة الموجودة في برنامج (Adobe's ColdFusion).
المصدر:
http://www.theregister.co.uk/201314/03//adobe_coldfusion_vulns_compromise_us_malware_catalog/
http://www.dslreports.com/forum/r28102110-US-National-Vulnerability-Database-Hacked

(26) A Practical Approach - Adventures in Security - Home (n.d.). Retrieved from http://adventuresinsecurity.com/blog/wp-content/uploads/2006/03/A_Practical_Appr

(27) https://nvd.nist.gov/

ثغرات نظام التشغيل:

ثغـرات نظام التشـغيل هي عبارة عن مشـكلات نظام التشـغيل التـي يمكن أن تمنح القراصنة الوصول إلى وظائف نظام التشـغيل والحسـابات. ولأن نظام التشـغيل هو لبنة البناء الأساسـية لجميع التطبيقات التي تعمل على النظام، يُطلب عادة من مسؤولي النظام تطبيق تصحيحات الأمان الخاصة بنظام التشغيل.

وتصدر شركة مايكروسوفت تصحيحات نظام التشغيل في يوم الثلاثاء الثاني من كل شهر. ويُعرف هذا اليوم بثلاثاء التصحيح أو الثلاثاء الأسـود للتأكيد على حقيقة أن على مسـؤولي النظـام تطبيق التصحيح على خـادم الاختبار (test server) وتحليـل تأثير التصحيح قبل تطبيـق التصحيح على خادم الإنتاج (production server). وإذا كان تصحيح الأمان يُعد حساساً ومهماً فإن شركة مايكروسوفت ستصدره بين أيام الثلاثاء. وهذا النوع من التصحيح يُعرف بتصحيح خارج النطاق (Out of Band Patch).

شكل (٦-١٣): عدد الثغرات المخترقة في عام ٢٠١١ حسب المورد

المورد	عدد الثغرات (٢٠١١)	عدد الثغرات العالية	عدد الثغرات المتوسطة	عدد الثغرات المنخفضة
جوجل (Google)	٢٩٩	١٧٣	١٢٥	١
أوراكل (Oracle)	٢٦٢	٤٦	١٦٣	٥٣
أبل (Apple)	٢٤٦	١٣٩	٨٩	١٨
مايكروسوفت (Microsoft)	٢٤٤	١٩٥	٤٦	٣
أدوب (Adobe)	١٨٩	١٥٣	٣٦	٠

ومـن بين أكـثر ١٠ ثغرات خارجية والمدرجة من قبل المورد الأمني (Qualys) في شـهر أغسـطس من عام ٢٠١٢، نذكر فيما يلي الثغرات الداخلية في نظام تشغيل مايكروسوفت. والثغرات الداخلية هي تلك التي يمكن لقراصنة الحاسب استغلالها بمجرد أن يجد له موطئ قدم في جهاز الضحية وعادة يتم ذلك من خلال اختراق حساب بامتيازات مستخدم عادي. وبعد ذلك يقوم قراصنة الحاسـب باستغلال هذه الثغرات للحصول على وصول بامتيازات مسؤول النظام ومن ثم يسيطر على جهاز الحاسب الآلي.

ثغرة تنفيذ التعليمات البرمجية عن بعد للخدمات الأساســية لمايكروسوفت إكس إم إل
-Microsoft XML core services remote code execution vulnerability (MS12)
:((and KB2719615 043

الخدمات الأساسية لمايكروسوفت إكس إم إل ٣,٠ و٤,٠ و٥,٠ و٦,٠ تصل إلى مواقع غير مهيأة في الذاكرة مما يسمح للمهاجمين عن بعد بتنفيذ رموز برمجية أو تتسبب في الحرمان من الخدمة عن طريق موقع إلكتروني متقن التصميم.

وتحــدث ثغرة تنفيذ التعليمات البرمجية عن بعد بســبب الطريقــة التي تتعامل فيها الخدمات الأساســية لمايكروســوفت إكس إم إل مع الأشــياء في الذاكرة. وقد تسمح الثغرة بتنفيذ تعليمات برمجية عن بعد إذا كان المستخدم يستعرض موقعاً إلكترونياً يتضمن بشكل خاص محتويات متقنة التصميم. والمهاجم الذي ينجح في اســتغلال هذه الثغرة قد يتمكن من الســيطرة الكاملة عــلى النظام المتأثر. وبعد ذلك يتمكــن المهاجم من تثبيت البرامج، واســتعراض البيانات وتغييرها وحذفها، أو إنشاء حسابات جديدة تتمتع بحقوق المستخدم كاملة. والمستخدم الذي لديه حساب بامتيازات قليلة (حساب مهيأ بحقوق محدودة على النظام) سيكون أقل تأثراً من المستخدم الذين يعمل بامتيازات مسؤول النظام[٢٨].

ثغرة انتحال الشــخصية من خلال شهادات ويندوز مايكروسوفت الرقمية غير المصرحة
Microsoft Windows unauthorized digital certificates spoofing vulnerability)
:(KB2728973

الشــهادات الرقمية غير المصرحة قد تؤدي إلى انتحال الشــخصية. وتُصدر الشــهادات بشكل غير منتظم من قبل مرجع التصديق بشركة مايكروسوفت (Microsoft Certificate Authority) لكنها أصبحت تُستخدم لتوثيق أجزاء من برنامج خبيث يدعى (Flame) وهو أحد البرمجيات الخبيثة المصممة على ما يبدو لاســتهداف التجسس وهو يشبه إلى حد كبير برنامج (Stuxnet). وقد اكتُشف البرنامج الخبيث (Flame) من قبل مختبرات كاسبرسكاي (Kaspersky Labs) في شــهر مايــو من عام ٢٠١٢ لكن على ما يبــدو أنه منتشر منذ عام ٢٠١٠.

(28) https://technet.microsoft.com/en-us/security/buIletin/ms12-043

ثغــرة تنفيذ التعليــمات البرمجية عن بعد لقشرة ويندوز مايكروســوفت (Microsoft Windows shell remote code execution vulnerability (MS١٢-٠٤٨)):

وتحدث هذه الثغرة بسبب الطريقة التي يتعامل بها ويندوز مع أسماء الملف والدليل. وهذه الثغرة قد تسمح بتنفيذ التعليمات البرمجية عن بعد إذا فتح المستخدم ملفاً أو دليلاً يحمل اسماً مصمماً بشكل خاص.

فإذا تم تســجيل الدخول بحقوق امتياز مسؤول النظام فإن المهاجم الذي يستغل هذه الثغرة بشــكل ناجح قد يتمكن من السيطرة الكاملة على النظام المتأثر. وبعد ذلك يتمكن المهاجم من تثبيت البرامج، واستعراض البيانات وتغييرها وحذفها، أو إنشاء حسابات جديدة تتمتع بحقوق المســتخدم كاملة. والمســتخدم الذي لديه حساب بامتيازات قليلة (حساب مهيأ بحقوق محدودة على النظام) سيكون أقل تأثراً من المستخدم الذين يعمل بامتيازات مسؤول النظام[٢٩].

ثغــرة رفع امتياز برامــج تعريف نظام نواة التشــغيل في ويندوز مايكروســوفت Microsoft Windows kernel-mode drivers elevation of privilege) :((047-vulnerability (MS12

وتحــدث ثغرة رفع الامتياز بســبب الطريقــة التي يتعامل بها نظام نواة التشــغيل في ويندوز مع تصميمات معينة للوحة المفاتيح. والمهاجم الذي ينجح في استغلال هذه الثغرة قد يتمكن من تشغيل تعليمات برمجية عشوائية في نظام نواة التشغيل. وبعد ذلك يتمكن المهاجم من تثبيت البرامج، واستعراض البيانات وتغييرها وحذفها، أو إنشاء حسابات جديدة تتمتع بحقوق مسؤول النظام كاملة[٣٠].

(29) https://technet.microsoft.com/en-us/security/buIletin/ms12-048

(30) https://technet.microsoft.com/en-us/security/buIletin/ms12-047

ثغــرة تنفيــذ التعليمات البرمجية عــن بعد لمكونــات دخول بيانات مايكروســوفت Microsoft Data Access Components remote code execution vulnerability) :((045-(MS12

وتحدث ثغرة تنفيذ التعليمات البرمجية عن بعد بســبب طريقة وصول مكونات دخول بيانات مايكروســوفت إلى كائن في الذاكرة تمت تهيئته بشــكل غير صحيح. والمهاجم الذي ينجح في اســتغلال هذه الثغرة قد يتمكن من تشغيل تعليمات برمجية عشوائية في النظام المســتهدف. وبعد ذلك يتمكن المهاجم من تثبيت البرامج، واســتعراض البيانات وتغييرها وحذفها، أو إنشاء حسابات جديدة تتمتع بحقوق المستخدم كاملة.

الإصدار الثاني من تصريحات قوانين الثغرات في شركة (Qualys)

نصف العمر: بلغ نصف حياة الثغرات الحرجة ٣٠ يوماً في جميع الصناعات. وبمقارنة الصناعات منفردة، جاءت الصناعة الخدمية بأقصر نصف حياة والتي بلغت ٢١ يوماً، وجاءت صناعة الموارد المالية في المرتبة الثانية بـ ٢٣ يوماً، وصناعة التجزئة جاءت في المرتبة الثالثة بـ ٢٤ يوماً، وصناعة التصنيع جاءت أخيراً بثغرة نصف حياة وصلت لـ ٥١ يوماً.

الانتشار: ٦٠٪ من الثغرات الأكثر انتشاراً وأهمية تُستبدل بثغرات جديدة سنوياً. وتشير الدراسات إلى أن هذا العدد قد زاد بنسبة ٥٠٪ منذ عام ٢٠٠٤. وأكثر المتضررين وفقاً لهذا الإصدار هي البرمجيات التالية: (MSFT Office) و (SP٢ ٢٠٠٣ Windows) و (Adobe Acrobat) و (Sun Java Plug-in).

الثبات: يشير هذا القانون إلى أن العمر الزمني لمعظم الثغرات - إن لم يكن كلها - غير محدود، ونسبة كبيرة من الثغرات لا تكون ثابتة أبداً. وقد تم توضيح هذا القانون باستخدام عينات بيانات من تصحيحات نظام تشغيل مايكروسوفت التالية: (001-MS08) و (007-MS08) و (015-MS08) و (021-MS08).

الاستغلال: ٨٠٪ من استغلال الثغرات تكون متوفرة خلال بضعة أيام من الإعلان العام عن الثغرة. وقد سجلت مختبرات (Qualys) ٥٦ ثغرة من ثغرات الاستغلال الفوري بما في ذلك ثغرة (RPC) والتي أنتجت (Conficker). وفي عام ٢٠٠٩، كان استغلال التصحيح الأول الذي صدر من مايكروسوفت (MS٠٩-٠٠١) متاحاً خلال ٧ أيام. وتضمن تصحيح الثلاثاء من شهر أبريل الاستغلالات المعروفة لأكثر من ٤٧٪ من الثغرات التي تم نشرها.

وتُعد تغييرات هذا القانون أكثر جدية من قوانين الإصدار الأول ١,٠ والذي صدر في عام ٢٠٠٤، كما أنه يقدم ٦٠ يوماً من الإرشادات المبسطة٣٠.

ثغرات تطبيقات الشبكة:

تطبيقات الشبكة تُدرِج نقطة أخرى للدخول إلى الأصول الأساسية التي تعرضها. منظمة (مشروع أمن تطبيقات الشبكة المفتوحة) (The Open Web Application Security Project) هي منظمة غير ربحية، ولها العديد من الفروع والمشاريع وتهدف لجعل تطبيقات شبكة الإنترنت أكثر أمناً. وكجزء من هذا المجهود تقوم المنظمة بنشر قائمة بأهم الثغرات الموجودة في تطبيقات الشبكة. وقد ناقشنا فيما مضى بعضاً منها عندما تحدثنا عن أنشطة التهديدات.

الحقن (Injection):

ويحدث الحقن عندما لا تقوم آلية تفسير الأوامر المرسلة من الجهاز العميل بالتحقق من الأوامر قبل تمريرها إلى التطبيق لتنفيذها. وعندما لا يتم التحقق من صحة المدخلات بالشكل الصحيح قد يقوم خادم الشبكة بمحاولة تنفيذ بعض الأوامر المقيدة والتي لا يجب تنفيذها. وفي الواقع فإن حقيقة أن المدخلات لا يتم التحقق من صحتها يعطي المهاجم «قشرة زائفة» للولوج إلى الخادم و/أو قاعدة البيانات.

ويتطلب منع الحقن الاحتفاظ بالبيانات التي يتم تمريرها من المصادر الخارجية (كما هو الحال في نماذج الشبكة) منفصلة عن أوامر واستفسارات الخلفية الحقيقية.

الطريقة المفضلة للتعامل مع هذه القضية هي استخدام واجهة برمجة التطبيقات (Application Programming Interface) والتي يستطيع المبرمج من خلالها تقييد نوع المدخلات المقبولة من الجهاز العميل. على سبيل المثال، يمكن للمبرمج أن يستخدم واجهة برمجة التطبيقات التي تقبل أمراً من كلمة واحدة مثل اقرأ (READ)، واكتب (WRITE)، وعدّل (MODIFY). وأي شيء آخر غير هذه الكلمات الرئيسية يتم تجاهله.

وإذا كانت هذه الطريقة غير متوفرة فإن على المبرمج أن يفحص التفسيرات بعناية كما عليه أن يقوم بتنظيف أي أمر من شأنه أن يسمح للجهاز العميل بالخروج عن البيئة المعهودة. على سبيل المثال، إذا كان الأمر المرسل من الجهاز العميل سيتم تمريره كمعيار إلى عبارة إس كيو إل (SQL) فإن على البرنامج أن يكتشف الخطأ في حال تمرير أي فاصلة منقوطة من قبل الجهاز العميل.

ويعـد الهجوم باسـتخدام آلية الحقن الأكثر شـيوعاً والأسـهل اسـتخداماً مثل (SQL Injection) أو (LDAP Injection).

هجمات البرمجة النصية للمواقع الإلكترونية المشتركة (cross-site scripting):

وتحدث هـذه الهجمات عندمـا يقوم التطبيـق بالتعامل مع معلومـات غير موثوقة وإرسالها إلى متصفح الإنترنت دون التحقق من صحتها. وتسمح هذه الهجمات للمهاجمين بتنفيذ الأوامر البرمجية في متصفح الإنترنت الخاص بالضحية مما يسـمح باختراق جلسـات العمل الخاصة بالمسـتخدم، وتشـويه مواقع الإنترنت، أو إعادة توجيه المستخدم إلى مواقع إلكترونية خبيثة. وفي حين أن الخوادم هي الأصول المستهدفة لهجمات الحقن (Injection) فإن الأهداف الرئيسـية لثغرات (البرمجة النصية للمواقع الإلكترونية المشتركة) هي العملاء المتصلون بالخوادم.

تزوير الطلب عبر المواقع الإلكترونية المشتركة (Cross-site request forgery):

عندما تجلس لاسـتخدام جهاز الحاسـب الآلي هنـاك احتمال كبير أن تقوم بتسـجيل الدخول إلى العديد من المواقع المختلفة مثل الفيسبوك (Facebook)، وشبكة مايكروسوفت (MSN)، والموقـع الاخبـار سي إن إن (CNN)، وغيرهـا. والمهاجم الذي يسـتخدم ثغرة (تزوير الطلب عبر المواقع الإلكترونية المشتركة) يعتمد على هذه الحقيقة لإرسال «طلبات» لخدمات التسجيل في تلك المواقع نيابة عنك.

وفي حـين أن هجـمات (البرمجة النصية للمواقـع الإلكترونية المشـتركة) «ترد» حمولة الخـادم مرة أخرى إلى العميل فإن هجوم (تزوير الطلب عبر المواقع الإلكترونية المشـتركة) يقوم بتنفيذ الأمر على الخادم نيابة عن العميل.

على سـبيل المثال، من وراء الكواليس ومن دون علمك قد يقوم المهاجم بإرسـال طلب باستخدام «بروتوكول نقل النص المتشعب» (HTTP) إلى الخادم بهذا الشكل:

http://somesite.com/change-password.php&user=jdoe?new-pwd=ilikepie

يتلقى خادم الشـبكة هذا الطلب، ويؤكد أنه تم تسـجيل دخول (jdoe)، ويقوم بتغيير كلمة المرور إلى (ilikepie).

الحماية غير الكافية لطبقة النقل (Insufficient transport layer protection):

وببساطة فإن ما سبق يؤكد أهمية التشفير المناسب لخادم الشبكة لأنه ليست جميع خوادم الشبكة تتطلب تشفيراً للبيانات. وفي الواقع فإن السبب الرئيسي للاتصال من خلال «بروتوكول نقل النص المتشعب» (HTTP) هو المواقع التي تتطلب تسجيل دخول من المستخدمين. وما لم تكن عملية تسجيل الدخول مشفرة فإن كامل المحتوى الذي سيُنقل، بما في ذلك بيانات اعتماد تسجيل دخول المستخدم، سيكون مرئياً للمهاجم الذي تمكن من الوصول إلى النظام.

ومن الأهمية بمكان استخدام لوغاريتم للتشفير بحيث تكون تلك اللوغاريتم صالحة ومطابقة للمعايير الحالية في مجال أمن المعلومات. وسنتطرق إلى موضوع التشفير في أحد الفصول القادمة.

وأخيراً فإن وجود شهادة موقعة من جهة معروفة ومخولة بالتوقيع، وتجديد تلك الشهادة حسب الحاجة يعد أمراً ضرورياً وخاصة بالنسبة للخوادم الإنتاجية. وتشير الشهادة الموقعة من جهة معروفة ومخولة بالتوقيع إلى عدم إمكانية الإنكار (وأن ما يدعيه الموقع الإلكتروني حقيقي) وهذا التشفير جدير بالثقة.

نموذج حالة-(Gozi):

عندما تُفكر في تهديدات أمن المعلومات، ربما تفكر في الأشخاص الأذكياء الذين يستخدمون ذكاءهم في محاولة مهاجمة جهازك الشخصي لتحقيق مكاسب شخصية. لكن هل تعلم أن هناك صناعة ناشئة تقوم بتطوير أدوات برمجية محترفة لمساعدة المهاجمين المبتدئين ليصبحوا قوة متخصصة هدفها الربح؟ في الثالث والعشرين من شهر يناير من عام ٢٠١٣ اتهم المدعي العام ثلاثة أشخاص وهم نيكيتا كوزمين (Nikita Kuzmin) من روسيا، ودينيس كالوفيسكس (Deniss Calovskis) من لاتفيا، وميهاي بانيسكو (Mihai Paunescu) من رومانيا بإنشاء وتوزيع برنامج خبيث أو حصان طروادة باسم (Gozi). وتم تخصيص هذا البرنامج لكل عميل بهدف مهاجمة المؤسسة المالية التي يختارها العميل. وتم القبض على هؤلاء الأشخاص الثلاثة في مناطق مختلفة من العالم خلال السنتين الماضيتين.

فيروس Gozi تم إصداره في عام ٢٠٠٥ وتم توزيعه على شكل ملف بي دي إف (PDF). وعندمـا يتم فتح الملف فإن الفيروس يُثبت نفسـه سراً، ولا يقوم بأي نشـاط خبيث حتى يتجنب التدقيق من برنامج مكافحة الفيروسات. وفي نهاية المطاف تم تثبيت هذا الفيروس عـلى أكثر من مليون جهاز حاسـب آلي في جميع أنحاء العـالم، بما في ذلك أكثر من ٤٠،٠٠٠ جهاز حاسب آلي في الولايات المتحدة.

الشـخص الذي ابتكر فـيروس (Gozi) انتقائي للغاية في اختيـار عملائه. فعندما يقوم العميـل بالدفـع لفريق الفيروس، سـيكون اختيار الأجهـزة المصابة متاحـاً لذلك العميل. وعند ذلك قد يختار العميل مؤسسـة مالية ليتم اسـتهدافها بناء على سلوكيات الاستخدام أو التفضيـلات المصرفية لمجموعة مـن الضحايا المتاحة له. ويقـوم فريق الفيروس بكتابة برمجيات مخصصة للعملاء والتي تعترض الاتصالات البنكية بين الضحايا والبنوك مما يسمح لعملاء الفيروس بأخذ بيانات اعتماد الحسابات البنكية.

ولتسـهيل التحويـلات المالية فـإن فريق الفيروس قـد أغرى بعض الأفـراد من خلال مخططـات تعبئة الظروف والتي من خلالها يحصل هؤلاء الأفراد على أموال من البنوك ثم يقومون بإرسالها بالبريد إلى العملاء مما يوفر مستوى من إخفاء الهوية للعملاء.

وفي حال إدانة فريق الفيروس فإن كل عضو من الأعضاء الثلاثة سيواجه عقوبة تصل إلى أكثر من ٦٠ عاماً في السجن.

المراجع:

http://www.justice.gov/usao/nys/pressreleases/January13/GoziVirusPR.php

http://krebsonsecurity.com/2013/01/three-men-charged-in-connection-with-gozi-trojan/

http://arstechnica.com/security/2013/01 /how-the-feds-put-a-bullet-in -a- bulIetproof-web-host/

http://krebsonsecurity.com/wp-content/uploads/2013/01/Calovskis-Deniss-S4-lndictment.pdf

http://krebsonsecurity.com/wp-content/uploads/2013/01/KuzminNikita-Information-1.pdf

http://krebsonsecurity.com/wp-content/uploads/2013/01/PaunescuMihai-Ionut-Complaint.pdf

الملخص:

رأينا في هذا الفصل أن التهديد يتكون من وسيط يقوم بأداء نشاط ما ضد الأصل. وبعد ذلك ناقشنا أهم الوسطاء وأهم الأنشطة التي يرجح أنك ستواجهها في مهنتك المستقبلية.

أسئلة مراجعة للفصل:

١. ما التهديد؟ أعطِ بعض الأمثلة.

٢. ما نموذج التهديد؟ ولماذا يُعد مفيداً؟

٣. باعتبار أن جهاز الحاسب الآلي المحمول الخاص بك أصلاً من الأصول، ارسم نموذج التهديد لهذا الأصل.

٤. ما وسيط التهديد؟ أعطِ بعض الأمثلة.

٥. ما الأنواع المختلفة لوسيط التهديد؟ كيف تطورت وانتشرت مع مرور الوقت؟

٦. اشرح الغش الإلكتروني النيجيري المعروف بـ (Nigerian Scam 419).

٧. ما مجموعات «الاختراق السياسية» (hacktivist)؟

٨. في رأيك ما المنظمة الموجودة في منطقتك والتي ستكون هدفاً محتملاً لهجمات مجموعات الاختراق السياسية (hacktivist)؟ ولماذا؟

٩. ما هي بعض دوافع الحكومات لرعاية أو تأييد الجرائم الإلكترونية؟

١٠. ما وسيط التهديد الداخلي؟ أعطِ بعض الأمثلة. وأي منها في اعتقادك الأكثر خطراً؟ ولماذا؟

١١.كيف تكون الإدارة العليا وسيطاً للتهديد من وجهة نظر أمن المعلومات؟

١٢.ما نشاط التهديد؟ وما هي بعض أنشطة التهديد الشائعة؟

١٣.ما نشاط التهديد الذي يمكن أن يصدر من المزود الخارجي للخدمات التقنية؟

١٤.ما هجوم القوة الغاشمة (brute-force attack)؟ وما الهدف التقليدي لهذا الهجوم؟

١٥.كيف يمكن للموظفين السابقين أن يصبحوا تهديداً؟ ما الذي تستطيع عمله لتقليل هذا التهديد؟

١٦.ما «التهديد الفوري» (zero-day threat)؟

١٧.ما تغيير التهديد (threat shifting)؟ وكيف يؤثر في عمل المختصين في أمن المعلومات؟

١٨.ما هجمات البرمجة النصية للمواقع الإلكترونية المشتركة (cross-site scripting)؟ وما الهدف التقليدي لهذه الهجمات؟

١٩.ما هي بعض أنشطة التهديد التي يمكن أن تصدر من البيئة (Environment)؟

٢٠.في رأيك ما أهم نشاط تهديد يمكن أن يصدر من البيئة في منطقتك؟

٢١.ما الثغرات؟

٢٢.ما العلاقة بين الثغرات والتهديدات؟

٢٣.في مجال أمن المعلومات ما الذي يُقصد بثلاثاء التصحيح (patch Tuesday)؟

٢٤. ما هي منظمة (مشروع أمن تطبيقات الشبكة المفتوحة) (The Open Web Application Security Project)؟ ولماذا هي مهمة للمختصين في أمن المعلومات؟

٢٥.بالرجوع إلى نموذج التهديد الذي طورته لجهاز الحاسب الآلي المحمول في السؤال الثالث أعلاه، في رأيك ما أهم وسيط تهديد وأهم نشاط تهديد لهذا النموذج؟

أسئلة على نموذج الحالة:

١. بناءً عــلى المعلومات الموجودة في نمــوذج الحالة، ما مقترحاتــك التي تعطيها لأحد أصدقائك حتى يكون آمناً أثناء تصفحه للإنترنت؟

٢. ما الاســتضافة الخالية من الثغرات أو التي تســمى بــ (bulletproof hosting)؟ ولماذا هي مهمة لمجرمي الإنترنت؟ (قد تحتاج للبحث في الإنترنت للإجابة عن هذا السؤال).

٣. ما مخالفات كل شــخص من الأشــخاص الثلاثــة الذين اتهمــوا بعلاقتهم بالفيروس (Gozi)؟

نشاط التدريب العملي-البحث عن الثغرات:

في هــذا التمرين ســتقوم بتثبيــت واختبار ماســح تقييم الثغــرات المفتوحة (Open Vulnerability Assessment Scanner) (يعــرف اختصاراً Open VAS) على آلة لينكس الافتراضية والتي ســبق الحديث عنها في الفصول الســابقة. ويتكون ماسح تقييم الثغرات المفتوحة من مجموعة من الأدوات التي تسمح لمسؤولي الأمن بمسح عدد كبير من الأنظمة بحثــاً عن الثغرات الشــبكية. ولمزيد من المعلومات يرجى الاطلاع عــلى الموقع الإلكتروني التالي:

www.openvas.org

ولتثبيت (OpenVas) افتح نافذة طرفية واذهب إلى حساب الجذر 'su':

```
[alice@sunshine ~] $ su-
Password: thisisasecret
```

بعد ذلك استخدم مدير تثبيت الحزم (YUM) وذلك لتثبيت الحزم المطلوبة:

```
[root@sunshine ~]# yum -y install openvas
Loaded plugins:  downloadonly, fastestmir-
ror, refresh-packagekit, security
Loading mirror speeds from cached hostfile
* atomic:  www4.atomicorp.com
* base:  mirror.flhsi.com
* extras:  mirror.cogentco.com
* updates:  mirrors.adams.net
Setting up Install Process
Resolving Dependencies
--> Running transaction check
---> Package openvas.noarch 0:1.05-.el6.
art will be installed
--> Processing Dependency:  openvas-admin-
istrator for package:  openvas-1.05-.el6.
art.noarch
--> Processing Dependency:  wmi for pack-
age:  openvas-1.05-.el6.art.noarch
--> Processing Dependency:  openvas-scan-
ner for package:  openvas-1.05-.el6.art.
noarch
--> Processing Dependency:  wapiti for
package:  openvas-1.05-.el6.art.noarch
```

وهذا الأمر سيقوم بتثبيت ٤٠ حزمة جديدة في النظام. وعند اكتمال التثبيت (والذي قد يستغرق بعض الوقت اعتماداً على اتصالك بالإنترنت) قم بتشغيل الأمر (openvas-setup) للبدء بعملية التهيئة، وقم بإدخال القيم الموجودة أدناه.

```
[root@sunshine ~]# openvas-setup
Openvas Setup, Version:  0.3
Step 1:  Update NVT's and SCAP data
Please note this step could take some time.
Once completed, NVT's and SCAP data will
be updated automatically every 24 hours


Updating NVTs....
Updating SCAP data...
[i] This script synchronizes a SCAP data
directory with the OpenVAS one.
[i] SCAP dir:  /var/lib/openvas/scap-data
[i] Will use rsync
[i] Using rsync:  /usr/bin/rsync
[i] Configured SCAP data rsync feed:
rsync://feed.openvas.org:/scap-data
OpenVAS feed server - http://openvas.org/
This service is hosted by Intevation GmbH -
http://intevation.de/
All transactions are logged.
Please report problems to admin@inteva-
tion.de
```

```
receiving incremental file list
./
COPYING          1493 100%     1.42MB/s
0:00:00 (xfer#1, to-check = 3032/)
COPYING.asc 198 100% 193.36kB/s
0:00:00 (xfer#2, to-check = 2932/)
debian.6.0.xml 980140 100% 652.02kB/s
0:00:01 (xfer#3, to-check = 2832/)
debian.6.0.xml.asc 198 100% 0.51kB/s
0:00:00 (xfer#4, to-check = 2732/)
...
Step 2:  Configure GSAD
The Greenbone Security Assistant is a Web
Based front end
for managing scans.  By default it is con-
figured to only allow
connections from localhost.

Allow connections from any IP? [Default:
yes] no
Step 3:  Choose the GSAD admin users password.
The admin user is used to configure
accounts,
Update NVT's manually, and manage roles.

Enter administrator username:  openvas-admin
Enter Administrator Password:  12345qwert
Verify Administrator Password:  12345qwert
ad main:MESSAGE:9806:  201314 19-01-h39.33
```

```
EST:  No rules file provided, the new user
will have no restrictions.
ad main:MESSAGE:9806:201314 19-01-h39.33
EST:  User openvas-admin has been success-
fully created.

Step 4:  Create a user

Using /var/tmp as a temporary file holder.
Add a new openvassd user
---------------------------------
Login:  openvas-user
Authentication (pass/cert) [pass] :  pass
Login password :  secret
Login password (again) :  secret

User rules
---------------
openvassd has a rules system which allows
you to restrict the hosts that openvas-
user has the right to test.
For instance, you may want him to be able
to scan his own host only.

Please see the openvas-adduser(8) man
page for the rules syntax.
```

```
Enter the rules for this user, and hit
ctrl-D once you are done:
(the user can have an empty rules set)
Ctrl-D
Login           :  openvas-user
Password         :  ***********
Rules           :
Is that ok? (y/n) [y] y
user added.

Starting openvas-administrator...
Starting openvas-administrator:   [ OK ]

Setup complete, you can now access GSAD
at:    https://<IP>:9392
```

ولا ستكمال عملية الإعداد ستحتاج أيضاً إلى تشغيل أمر إضافي. ونحيطك علماً بأن هذا الأمر الإضافي سيستغرق ٢٠ دقيقة أو أكثر لإتمامه لذا يرجي التحلي بالصبر.

```
[root@sunshine tmp]# /opt/book/threats/
scripts/finish_openvas_setup This pro-
gram completes the OpenVAS configuration
process.
Stage 1:  Loading and processing plugins
Processing 57744 plugins.  Please be
patient.  This will take 15 minutes or
more depending on your hardware.
Starting openvas-scanner:  base gpgme-
Message:  Setting GnuPG homedir to '/etc/
openvas/gnupg' base gpgme-Message:  Using
OpenPGP engine version '2.0.14'

Stage 2:  Building the OpenVAS-Manger
database
This will take 1015- minutes depending on
your hardware.
done.

Stage 3:  Starting services
Stopping openvas-manager:
Starting openvas-manager:        Stopping
openvas-administrator:
Starting openvas-administrator:

Setup complete.  Please open Firefox and
go to https://www.sunshine.edu:9392
```

افتح نافـذة المتصفح واذهب إلى الموقع الإلكـتروني التـالي (٩٣٩٢:https://www.sunshine.edu). سـوف يُعرض لك شـهادة تحذير. ويظهر هذا التحذير لأن إنشاء الشهادة تم خلال عملية تثبيـت (OpenVAS) لذا فإن المتصفح فايرفوكـس (FireFox) لا يتمكن من التحقق من الشهادة من جهة خارجية.

انقر على السـهم المجاور لعبارة «أنا أتفهم المخاطر» (I Understand the Risks) ثم انقر على زر «إضافة استثناء» (Add Exception). سيتم عرض الشاشة الموضحة في الشكل (٦-١٤). ولقبـول الشـهادة تأكد من اختيـار مربع الاختيار «حفظ دائم لهذا الاسـتثناء» (Permanently store this exception) وانقر على زر «تأكيد استثناء الأمان» (Confirm Security Exception).

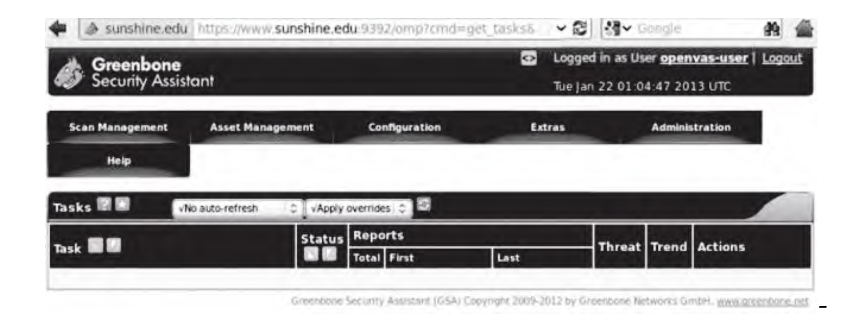
سـيتم عرض شاشـة دخول لتطبيـق (Greenbone Security Assistant) والذي يُعد واحـداً من العديد من التطبيقـات التي تُمثِل نظـام (OpenVAS). ويقوم هذا التطبيق بتوفـير واجهة رسـومية لكافة ميزات المسـح في نظام (OpenVAS). ولتسـجيل الدخول اسـتخدم حسـاب (openvas-user) وكلمة المرور التي أنشـأتها أعلاه. وتظهر الشاشـة الرئيسية لتطبيق (Greenbone Security Assistant) في الشكل (٦-١٥).

اختر «مهمة جديدة» (New Task) من قائمة «إدارة المسـح» (Scan Management). سوف يتم عرض الشاشة في الشكل (٦-١٦). ولإنشاء مهمة مسح جديدة املأ حقل «الاسم» (Name)- لقد سـمينا هذه العينة (myScan) لكن الاسـم الفعلي ليس مهماً. قم بتغيير القائمة المنسدلة من «ضبط المسح» (Scan Config) إلى «مسح كامل وعميق جداً» (Full and very deep ultimate) وذلـك حتـى يتم مسـح جميع الثغـرات المتضمنة في نظام (OpenVAS). وبإمكانـك تـرك الحقول الأخـرى في قيمها الافتراضية. انقر على «إنشـاء مهمة» (Create Task) لاستكمال عملية الضبط.

الشكل (٦-١٤): استثناء لشهادة من المتصفح فايرفوكس

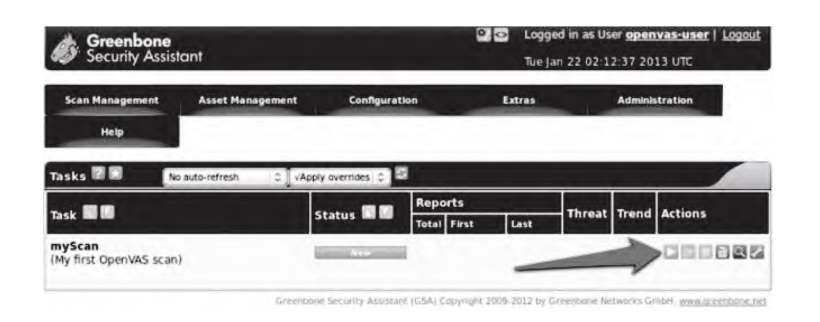


الشكل (٦-١٥): الشاشة الرئيسية لتطبيق (Greenbone Security Assistant)



الشكل (٦-١٦): تكوين مهمة جديدة

الشكل (٦-١٧): البدء في مسح جديد



وبمجرد إنشاء المهمة سيتم عرض المهمة على الشاشة. ولبدء عملية المسح انقر على زر البدء (انظر الشــكل ٦-١٧). ســيتم تغيير حالة المهمة من «جديد» (New) إلى «مطلوب» (Requested). وســوف يســتغرق ٥-١٠ دقائق لإكمال عملية المســح، وبإمكانك تحديث صفحة فايرفوكس للتحقق من الوضع الحالي.

وعند اكتمال عملية المسح انقر على زر التفاصيل (انظر الشكل ٦-١٨).

صفحة تفاصيل المســح تقدم لك لمحة عامة عن المســوحات التي تم تشــغيلها ونتائجها. ولعرض تقرير المسح الذي تم الانتهاء منه فقط، انقر على زر التفاصيل لفتح «صفحة التقرير» (Report Page). وفي صفحــة التقريــر يمكنك عرض نتائج المســح أو تحميل التقرير بصيغ متنوعة. ولتحميل التقرير اختر صيغة الملف وانقر على زر تحميل (انظر الشكل ٦-١٩).

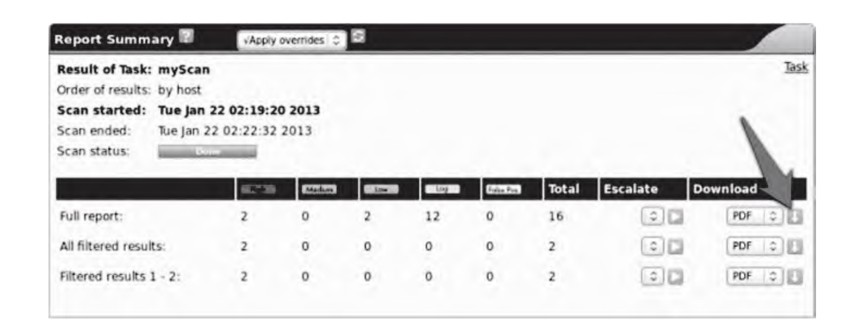
النتائج المطلوب تسليمها:

احفظ التقرير كاملاً باسم (openvas_report.pdf) وأرسله إلى أستاذ المادة.

الشكل (٦-١٨): عرض تفاصيل المسح



الشكل (٦-١٩): صفحة التقرير



تمرين التفكير النقدي-خطط الحرب الإلكترونية في العراق في عام ٢٠٠٣:

في شهر أغسطس من عام ٢٠٠٩، ذكرت صحيفة نيويورك تايمز أنه في عام ٢٠٠٣، عندما كانت الولايات المتحدة تخطط لحرب العراق، وضعت وكالات الاستخبارات ووزارة الدفاع الأميركية خطة لإطلاق هجوم إلكتروني بهدف تجميد الحسابات المصرفية التابعة لصدام حسين. وكانت تحتوي تلك الحسابات المصرفية على مليارات الدولارات وكانت تستخدم لدفع رواتب أفراد الجيش وشراء اللوازم الأخرى. وفي حال نجاح تلك الهجمات الإلكترونية فإنها ستشل قدرة صدام حسين على شن حرب بالأسلحة التقليدية.

وكما ذكرت صحيفة نيويورك تايمز، فإن المسؤولين المعنيين بتطوير خطط الهجمات الإلكترونية كانوا واثقين من قدرتهم على تنفيذ تلك الهجمات إلا أنهم لم يحصلوا على موافقة لتنفيذ خططهم. وكان المسؤولون في إدارة الرئيس بوش يخشون من الأضرار الجانبية لتلك الهجمات، كالآثار التي قد تحدث على الحسابات التي يملكها الأفراد الآخرون، في حال أن أي جزء من الهجوم الإلكتروني لم يذهب وفقاً للخطة. وهذا يمكن أن يخلق فوضى مالية في جميع أنحاء العالم، بدءاً من الشرق الأوسط مروراً بأوروبا وحتى الولايات المتحدة.

كان ذلك في عام ٢٠٠٣. ومنذ ذلك الحين تطورت التقنية وأصبحت الحرب الإلكترونية بشكل متزايد جزءاً من الترسانة العسكرية. وحتى خلال الحرب على العراق في عام ٢٠٠٣ شمل الهجوم العسكري تعطيل شبكات الهاتف داخل العراق. وهذا أثر بشكل مؤقت في خدمات الهاتف المدنية في الدول المجاورة للعراق. ومع ذلك فقد عُدّ هذا الضرر مقبولاً في ذلك الوقت. لكن الضرر غير المؤكد للهجمات الإلكترونية والذي يُعتقد أن يكون خارج السيطرة لم يكن مقبولاً. ومنذ ذلك الحين تشعر الولايات المتحدة بالارتياح لاستخدام الهجمات الإلكترونية في المستقبل لتحقيق أهدافها كما هو موثق بشكل جيد في حالة فايروس (Stuxnet).

المراجع:

Markoff, J. and Shanker, T. «Halted '03 Iraq plan illustrates U.S. fear of cyberwar risk,» New York Times, August 1, 2009

أسئلة على تمرين التفكير النقدي:

١. مـا هي بعـض الطرق (وإن كانـت غير مُحتملـة) التي يمكن مـن خلالها للهجوم الإلكتروني المقترح على الحسابات المصرفية لصدام حسين أن يضرك؟

٢. ما هي بعض الطرق التي يمكن للهجوم الإلكتروني على هدف عسكري أن يضر المدنيين؟

٣. أحد القيود العسـكرية المنبثق عن اتفاقيات جينيف وميثاق الأمم المتحدة يُسـمى الملاءمة (proportionality)، ويُقصد به تلاؤم العقاب مع الجريمة. وبأخذ مخاطر الهجمات الإلكترونية التي تم تحديدها في الأسئلة السابقة بعين الاعتبار، هل تعتقد أنه من المرجح أن تُسـبب الهجمات الإلكترونية ضرراً غـير ملائماً للمدنيين أكثر من الأسلحة التقليدية؟

تصميم حالة:

لدى مكتب الدعم الفني في كلية الهندسـة في ولاية الشـمس المشرقة امتيازات خاصة حيـث يتمكن من إصلاح مشـكلات وصول المسـتخدم من خلال تجاوز إجـراءات تحكم الدخول العادية.

وقد تتسـاءل كيف حدث هذا؟ قبل سـنوات كان أحد أسـاتذة الهندسـة الكهربائية، والذي يحظى باحترام كبير في الكلية، غير قادر على إرسـال طلب منحة لأنه أقفل حسـابه الرسـمي بالخطأ خلال عطلة نهاية الأسـبوع. وأدى ذلك إلى الحزن الشـديد لعميد الكلية ورئيس القسـم. وكحلٍ «مؤقت» لهذه المشـكلة مُنح الطلاب العاملـون في مكتب الدعم الفني امتيازات مسؤول النظام لمجال شبكة (كلية الهندسة) حتى يتمكنوا من تغيير كلمات المرور وفتح الحسابات دون إزعاج أعضاء هيئة التدريس والموظفين.

وبعد سـنوات أصبح ما يسـمى بـ (الحل المؤقت) حلاً دائماً وأصبح جميع المستخدمين يتوقعون استجابة سريعة خلال عطلة نهاية الأسبوع.

وفي صباح أحد أيام السـبت، قرر آدم، وهو طالب جديد يعمل في مكتب الدعم الفني، تثبيت برنامج (BitTorrent)، وهو أمر يخالف سياسـية الكلية. وفي وقت لاحق من ذلك

الأسبوع، أُجري تحقيق بسبب بطء أجهزة الحاسب الآلي. وأدى ذلك التحقيق إلى اكتشاف تركيب الروبوت الشبكي (botnet) في معظم أجهزة الحاسب الآلي في الكلية. وبعد أيام من التحقيق تم اكتشاف مصدر تثبيت الروبوت الإلكتروني عندما تم العثور على مُسجل مفاتيح (keylogger) في الجهاز الذي يستخدمه آدم. وقد قام آدم دون قصد بتثبيت برامج ضارة على الجهاز أثناء تثبيته لبرنامج (BitTorrent)، كما أن مسجل المفاتيح قد التقط بيانات اعتماد حساب آدم.

وقد طلب منك عميد الكلية أن تكتب تقريراً عن هذا الحادث وتضعه على مكتبه في أسرع وقت ممكن بحيث يتضمن التقرير توصيات تمنع مثل هذه الحوادث في المستقبل.

أسئلة على تصميم الحالة الأمنية:

١. اذكر التهديدات والثغرات التي سمحت لهذه المشكلة بالحدوث.

٢. قم بتصنيف جميع الأحداث التي وجدتها في (١) أعلاه بما في ذلك:

- الأصول المتأثرة بما في ذلك تصنيف الأصول وتحديد خصائصها.
- وسيط التهديد (بما في ذلك الداخلي والخارجي والشريك).
- نشاط التهديد (كالنوع).
- الثغرة المستخدمة.

٣. ما التوصيات التي ستقدمها للعميد للتغلب على هذه المشكلة في المستقبل؟

٤. في رأيك ما الذي ينبغي القيام به مع آدم وهو الطالب الذي تم تعيينه مؤخراً في مكتب الدعم الفني؟

الفصل السابع

ضوابط التشفير

نظرة عامة:

التشـــفير هو أحد تقنيات التشـــغيل الأساســـية المُســـتخدمة في مجال أمن المعلومات. فالتشـــفير يساعد بشكل أســـاسي على الحفاظ على سرية المعلومات. ومن خلال تطبيقات مُبتكرة يمكن للتشـــفير أيضاً التأكد من تكامل المعلومات والتأكد من هوية المُرســـل. وكل العمليـــات التجاريـــة التي يتم إجراؤها عبر الإنترنت تســـتخدم التشـــفير للحفاظَ على أمن المعلومات. ويضمن التشفير أن المعلومات المالية، مثل أرقام بطاقات الائتمان، المرسلة عبر شبكة الإنترنت لا يتم سرقتها أثناء عملية النقل. وفي كثير من الحالات فإن التشفير ليس أمراً مناسباً فقط بل هو أمر مطلوب بموجب القانون الفيدرالي. لذا فإن التشفير جزء أساسي من البنية التحتية التجارية الحديثة. وفي هذا الفصل ســـنقدم أساســـيات تقنيات التشفير. كما ســـنناقش التحديات التشـــغيلية التي تواجه تطبيق التشفير والحلول التي وضعت لمواجهة هذه التحديات. وفي نهاية هذا الفصل يجب أن تعرف:

- أنواع التشفير الثلاثة الأكثر شيوعاً واستخداماتها المناسبة.
- معايير التطبيق العملية لتقنيات التشفير المستخدمة في تبادل المعلومات.
- استخدام البديل لتقنيات التشفير وذلك للتحقق من الهويات على شكل تصديقات.
- البنية التحتية للمفتاح العام (PKI) والتي تم تطويرها لجعل التشفير عملية مناسبة وعملية.

مقدمة:

مـــاذا نتوقع عندمـــا نقوم بإرســـال المعلومات عبر الإنترنـــت؟ بالتأكيـــد نريد أن تصل المعلومات إلى الشـــخص المُرســـل إليه[1]. لكـــن هل ذلك يكفي؟ ماذا إذا كانت الرســـالة: «ليس لدي المال لدفع فاتورة الرســـوم الدراسية لهذا الفصل الدراسي. يُرجى تحويل ١٠٠٠ دولار لحسابي الجاري رقم (#٠٠٠٠١٠١٠١٠) في الاتحاد الائتماني، ورقم التوجيه المصرفي هو (١٢٣٤٥٦٧٨٩). وفي حال وجود أي صعوبة فإن كلمة السر هي (hello123)».

(١) للاطلاع على معلومات تمهيدية حول كيفية إرسال المعلومات وتلقيها على الشبكات الحاسوبية انظر الملحق.

في عالم أمن المعلومات من الشـائع استخدام أسـماء أليس (Alice) وبوب (Bob) على أنهما المرسـل والمستقبل للرسـائل وذلك عند مناقشة الاتصالات الآمنة[٢]. في مثالنا السابق افـترض أن أليس (Alice) تريد إرسـال الرسـالة لبـوب (Bob). ما المميـزات التي ترغب فيهـا أليس (Alice) في هـذا التواصل؟ أولاً ترغب أليس (Alice) أن تصل الرسـالة لبوب (Bob). ثانيـاً قد ترغب أليس (Alice) أن يكون بوب (Bob) هو الشـخص الوحيد الذي يفهم الرسـالة حتى لو تمكن صديقاتها من رؤية أو سماع المحادثة. (وبالنتيجة، من يرغب أن يعلم أصدقاؤه بأنه مُفلس؟). وعند اسـتلام الرسـالة فمن المرجح أن يريد بوب (Bob) تأكيداً أن الرسـالة جاءت من أليس (Alice). وقد يسعى بوب (Bob) للحصول على تأكيد أن محتويات الرسـالة صحيحة. وفي الواقع فإن التشـفير لا يقوم بإرسال الرسالة بل يعطينا كل الميـزات المطلوبـة في التواصل بين أليس (Alice) وبـوب (Bob). وبالاقتباس من أحد الإعلانات التجارية المشـهورة، هناك أشـياء لا يسـتطيع أمن المعلومات القيام بها، ولهذه الأشياء يوجد التشفير.

وعلى مستوى عالٍ من التوضيح، فإن التشفير يحول الرسالة إلى شكل يتمكن من خلاله مسـتقبل الرسالة فقط من فك الشـفرة مما يوفر السرية. وأثناء فك الشفرة فإن مُستقبِل الرسالة يسـتطيع اكتشاف إذا تم تعديل الرسالة أثناء الإرسـال مما يضمن تكامل الرسالة. ولأن التشـفير مفيد جداً فإنه يُسـتخدم في أمن المعلومات بشكل مناظر لاستخدام السكين المتعددة الأغراض المعروفة بسكين الجيش السويسري. وإذا كان أمن المعلومات متضمناً في موضوع ما فإن هناك احتمالاً كبيراً بأن عملية التشفير أيضاً متضمنة بشكل أو بآخر.

أساسيات التشفير:

يتم التشـفير من خلال علم التشفير (cryptography). وكلمة (cryptography) هي كلمة مركبة تتكون من كلمتين يونانية الأصل: الأولى (κρυπτο) (crypto) وتعني مخفي والثـاني (γραφη) (graphy) وتعني الكتابـة و(cryptography) تعني الكتابة الخفية.

---

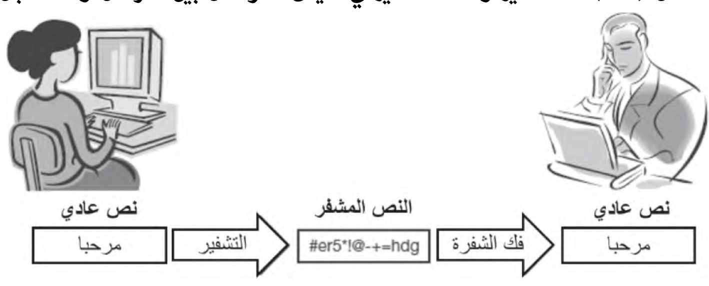
(٢) ويدعي موقع ويكيبيديا (Wikipedia) أن هذه الأسماء تم استخدامها لأول مرة من قبل رون ريفست (Ron Rivest) في دراسته التي تناقش بروتوكول التشفير الذي يحمل اسمه (RSA protocol). وسنتحدث بتفصيل أكبر عن هذا البروتوكول في وقت لاحق في هذا الفصل (https://en.wikipedia.org/wiki/Alice_and_Bob).

ووفقـاً لقامـوس مصطلحـات (ATIS telecom)، وهـو المصدر الموحـد للتعريفات في هذا الكتاب، فإن التشـفير (encryption) يُعرف بأنـه الكتابة السرية للبيانات (cryptography) وتحويلهـا لإنتاج نص مشـفر (ciphertext). ويقدم لنا هذا التعريـف مصطلحين جديدين هما: (cryptography) و(ciphertext). لقد ناقشـنا فيما سبق أن (cryptography) تعني الكتابة الخفية. وبشكل رسمي أكثر واعتماداً على قاموس مصطلحات (ATIS telecom) يمكن تعريف (cryptography) بأنها الفن أو العلم الذي يقوم بتسليم معلومات لا يمكن فهمها مع إمكانية اسـتعادة المعلومات المشفرة في شكل مفهوم. أما (ciphertext) فتعني النص المشفر غير المفهوم للقارئ. واشـتقاق كلمة (ciphertext) يسـتند إلى الكلمـة العربية صفر (cifr) والتي تعني لا شيء. وفي وقت لاحق استُخدمت كلمة (cifr) لتمثيل الرقم (٠). وعند الطرف المُستقبل للرسالة فإن فك التشفير (decryption) يُستخدم لحل رموز (decipher)[٣] النص الخفي.

وجميع هذه الأنشطة موضحة في الشكل (٧-١) والذي يعرض العملية الشاملة للتواصل الآمن بين أليس (Alice) وبوب (Bob).

ومن المفيد أن نتذكر أن التشفير يمكنه القيام بالكثير. فكما أن آلة قطع المسامير ستكسر أي قفل، فإن المسـتخدم الذي يكون على اسـتعداد لمُشـاركة كلمة المـرور الخاصة به مع الآخرين سيؤثر بدوره في أي نظام تشفير.

الشكل (٧-١): التشفير وفك التشفير في سياق التواصل بين المرسل والمستقبل



(٣) هل تفهم الآن اشتقاق هذه الكلمة؟ كلمة (De-cipher) أو (de-zerofy) تعني تحويل الرسالة التي تبدو دون معنى إلى رسالة ذات معنى.

النشأة:

أول حالة موثقة لعملية تشفير كانت للإمبراطور الروماني يوليوس قيصر (١٠٠ قبل الميلاد -٤٤ قبل الميلاد). ويوضح الشـــكل (٧-٢) مقتطفاً من العمل المترجم الذي يصف أســـلوب التشـــفير المتبع آنذاك[٤]. ومن ثم «إذا كان هناك حالة تتطلب السرية فإنه كان يســـتخدم الحروف الأبجدية بطريقة لا يُفهم منها ولا كلمة واحدة. وكانت الطريقة لفك تلك الرسائل من خلال استبدال الحرف (d) بالحرف (a) وكذلك الحروف الأخرى على التوالي».

الشكل (٧-٢): مرجع شفرة قيصر

JULIUS CÆSAR. 47

before him: for they are diſtinguiſhed into pages in the form of a pocket-book; whereas the Conſuls and Generals, till then, uſed conſtantly in their letters to continue the line quite acroſs the ſheet, without any folding or diſtinction of pages. There are extant likewiſe ſome letters from him to Cicero, and others to his friends concerning his domeſtic affairs; in which, if there was occaſion for ſecreſy, he uſed the alphabet in ſuch a manner, that not a ſingle word could be made out. The way to decipher thoſe epiſtles was to ſubſtitute *d* for *a*, and ſo of the other letters reſpectively. Some things likewiſe paſs under his name, ſaid to have been written by him when a boy, or a very young man; as the Encomium of Hercules, a tragedy entitled Œdipus, and a collection of Apophthegms; all which Auguſtus forbid to be publiſhed, in a ſhort and plain letter to Pompeius Macer, whom he had appointed to direct the arrangement of his libraries.

LVII. He was a perfect maſter of his weapons, a complete horſeman, and able to endure fatigue beyond all belief. Upon a march, he uſed to go at the head of his troops, ſometimes on horſeback, but oftener on foot, with his head bare in all kinds of weather. He would travel in a poſt-chaiſe at the rate of a hundred miles a day, and paſs rivers in his way by ſwimming, or ſupported with leathern bags filled with wind, ſo that he often prevented all intelligence of his approach.

LVIII. In his expeditions, it is difficult to ſay whether his caution or boldneſs was moſt conſpicuous. He never marched his army by a rout which was liable to any ambuſh of the enemy, without having previouſly examined the ſituation of the places by his ſcouts. Nor did he paſs over

وهكـــذا فإنه في شـــفرة قيصر يتم اســـتبدال كل حرف بالحرف الـــذي يليه بثلاثة أماكن إلى اليمـــين تبعاً لترتيـــب الحروف الأبجدية. ومن ثم فإن ((A) ß (D)،(B) ß (E)،...،(Q) ß (T)،...،(W) ß (Z)،(X) ß (A)،(Y) ß (B)،(Z) ß (C)). وفي حين يستخدم قيصر الاستبدال

(4) Alexander Thomson, M.D. (M.DCC.XCVI (1796)). The lives of the first 12 Caesars, translated from the Latin of C. Suetonius Tranquillus: with annotations and a review of the government and literature of the different periods. London, U.K., G.G. and J. Robinson, Paternoster-Row

بناء على ثلاثة أحرف لليمين، بإمكاننا بسهولة استخدام استبدال آخر. على سبيل المثال الاستبدال بناء على أربعة أحرف لليمين سيعطينا نظاماً للتشفير مثل (F) ß (B)،(E) ß (A).

وهذا المثال المبسط يوضح مفهوماً في غاية الأهمية في التشفير ألا وهو مفهوم المفاتيح. وفيما بعد سنتكلم عن المفاتيح وأهميتها.

وفي الواقع يمكن تعميم الطريقة أبعد من ذلك. فالحروف ليس من الضروري استبدالها بنفس عدد الأماكن لأن تعيين حرف معين إلى حرف آخر سيعمل كنظام للتشفير. على سبيل المثال، (B) ß (C)، (X) ß (B)،(H) ß (A) سيكون أيضاً فعالاً. وفي الواقع فإن نظام التشفير القائم على استبدال حروف منفردة بحروف أخرى بهدف التشفير يُعرف في أدبيات الأمن بالاستبدال الأحادي الأبجدي (mono-alphabetic substitution).

يوضح هذا المثال لَبِنة مهمة جداً من لَبنات العديد من تقنيات التشفير وهي الاستبدال (substitution). وسنوضح قريباً كيفية استخدام الاستبدال في تقنيات التشفير الحديثة.

في حين أنّ التشفير يضمن سرية البيانات إلا أن تلك السرية لا تكون مرغوباً فيها دائماً. فهناك برمجيات خبيثة تُستخدم حالياً لتشفير بيانات الحاسب الآلي وتبقيها مشفرة حتى يتم دفع مبلغ مالي إلى قراصنة الحاسب. وهذا النوع من البرمجيات الضارة يُسمى ببرمجيات الفدية (ransomware). ويشكل التشفير مشكلة لخبراء الأمن المشاركين في الأدلة الجنائية للبيانات وذلك لأن التشفير يحجب تفاصيل الحادث الأمني. كما أن التشفير يعيق استخدام جدران الحماية النارية (firewalls) وأجهزة الشبكة الأخرى بناءً على التدقيق العميق لحزم البيانات من أجل السماح بتدفق بيانات محددة أو منعها. وإذا كانت البيانات الموجودة في الحزمة مشفرة فإنه لا يمكن تدقيقها.

تحليل متطلبات التشفير:

ما المتطلبات التي يجب أن تتوافر في التشفير الجيد؟ بصفة عامة تشترك تقنيات التشفير في العديد من الخصائص مع الأقفال المادية للأبواب، وتقنيات التشفير الجيدة مماثلة للأقفال الجيدة في نواحٍ كثيرة. ماذا نتوقع في الأقفال الجيدة؟ أولاً، نتوقع أن تكون سهلة الاستخدام لأصحابها. ثانياً، نتوقع أن تكون صعبة الكسر للدخلاء. وفي حين أن معظم الأقفال يمكن في نهاية المطاف كسرها، إلا أن الأقفال تحتاج إما إلى أن تستغرق وقتاً طويلاً للكسر مما يلفت انتباه المتفرجين، وإما إلى أن تكون مكلفة للغاية للكسر لكي تستحق كل هذا الجهد.

وتشــترك تقنيات التشــفير الجيدة أيضاً في هــذه الخصائص. ونتوقــع أن تكون تقنية التشــفير الجيدة سهلة الاستخدام لمرسلي ومستقبلي المعلومات المصرح لهم. كما نتوقع أن المستخدمين غير المصرح لهم سيأخذون الكثير من الوقت لكسر التشفير بحيث أنهم إما أن يستسلموا أو أن تُلاحظ أفعالهم قبل أن ينجحوا.

وفي مجال أمن المعلومات يتم قياس الجهد من حيث المتطلبات الحسابية حيث يتطلب نظام التشــفير الجيد الحد الأدنى من الحســابات من قبل المســتخدمين المصرح لهم بقراءة وكتابة البيانات، ولكن في الوقت نفســه يتطلب من المستخدمين غير المصرح لهم عدد كبير ومستحيل من العمليات الحسابية.

ويجب أن يهتم مبتكرو تقنيات التشــفير بحقيقة أن المتســللين يمكن أن يكونوا أذكياء جداً في محاولتهم لكسر أنظمة التشــفير. ويُطلق على فن كسر النص المشفر «تحليل الشــفرات» (cryptanalysis). على سبيل المثال في حال استخدام الاستبدال الأحــادي الأبجــدي (mono-alphabetic substitution) اعتــماداً عــلى الأبجدية الإنجليزيــة، يمكننا اســتخدام حقيقة أن بعض الحروف تُعد أكثر شــيوعاً من غيرها (مثــلاً، e > t > a > I > o > n > s > h > r > d > l > u) وذلــك لتخمــين نظــام التشــفير ببســاطة من خلال عد الحروف وتردداتها النسبية. وبهذه المعرفة تشير التقديرات إلى أنه يمكن كسر نظام الاســتبدال الأحادي بمجموعة من ٦٠٠ رمز مشــفر تقريباً. وإذا تم تخمين الكلمات المُحتملة ســنحتاج فقط إلى ١٥٠ حرفاً. وقد يحاول المهاجمون إرسال نص انتقائي لمعرفة كيف يعمل التشــفير. على ســبيل المثال، إرســال (BAT) و (CAT) يمكن أن يشير إلى كيفيــة أن التغيــير في حرف واحد في النص يؤثر في مخرجات التشــفير مما يعطي بعض التلميحات لكسر نظام التشفير.

المفاتيح:

كما أنه ليس من الســهل التوصل لأقفال تكون ســهلة واقتصادية للمستخدمين المرخص لهم وفي الوقت ذاته صعبة الكسر للمســتخدمين غير المرخص لهم، فإنه ليس من الســهل كذلك التوصل إلى تقنيات تشــفير بخصائص مماثلــة. وبالنظر في محيطنا، كم عدد الأنواع

المختلفة للأقفال حولنا؟ هناك أقفال بمفاتيح، وأقفال مدمجة، وأقفال بيومترية، وربما بعض الأنــواع الأخرى مــن الأقفال. وهذه بعض أنواع الأقفال المســتخدمة لتأمين جميع الأبواب والخزائن في العالم. وبالمثل فإن بعضاً من تقنيات التشفير تؤمن جميع المعلومات في العالم.

وبالعــودة إلى مثال الأقفال، فإذا كان هناك بعض من أنواع الأقفال الجيدة، كيف يمكننا استخدام نفس نوع القفل لتأمين جميع المنازل في الحي؟ وبالنتيجة فإنه ليس من المفيد أن تكون طريقة فتح باب واحد تؤدي لفتح جميع الأبواب في الحي. وهذا يقودنا إلى المفاتيح، بمعنــى أن الأقفال تكون مُميَزة من خلال مفاتيحهــا. أي أن المفتاح الذي يفتح قفلاً معيناً يكون خاصاً بذلك القفل.

التشابه بين التشفير ونوع القفل يدعى خوارزمية التشفير (cryptographic algorithm) أو اختصاراً خوارزمية. وخوارزمية التشفير هي تسلسل من الخطوات المستخدمة والمحددة بشــكل جيد لوصف عمليات التشفير. وعموماً سنُطلق عليهم «خوارزميات». وحتى الآن قد تم اكتشــاف بعــض الخوارزميات الجيــدة والتي تحتوي عــلى كل الخصائص المرغوب فيها. وتُعد كل حالة من حالات الخوارزمية المُختارة فريدة من خلال مجموعة من الأرقام الفريدة والتي تدعى «مفتاح» (key). وفي ســياق التشــفير فإن المفتاح سلسلة من الرموز التي تتحكم في عمليات تشفير وفك التشفير. والمستخدمون الذين يملكون المفتاح الصحيح يمكنهم بســهولة تبادل المعلومات معاً. وسيستغرق تخمين المفتاح الصحيح وقتاً طويلاً من المُتصنتين.

مــا خصائص المفتاح الجيــد؟ كما ذكرنا مــراراً وتكراراً، يجب أن يكــون المفتاح الجيد صعب التخمين. وفي ســياق التشفير يتم كسر المفاتيح ببساطة عن طريق استخدام مفاتيح مختلفــة حتى يتم العثور على المفتاح الصحيح. فإذا اســتخدمنا مفاتيح من خانة واحدة، ســيكون لدينا ١٠ مفاتيح ممكنة (٠, ١، ...، ٩). وإذا كان المتســلل يحتاج إلى ثانية واحدة لتجريــب مفتــاح واحد، فإنه ســيحتاج إلى ١٠ ثوان لتخمين المفتــاح الصحيح. وإذا كانت العملية مُكررة عدة مرات، فإن متوسط الوقت سيكون نصف ذلك، أي ٥ ثوان. وهذا لأنه في بعــض الأحيان يكون التخمين الأول صحيحاً، وفي حالات أخرى يكون التخمين الســادس يكون صحيحاً، وهكذا. ولتحســين الوضع الأمني يمكننا استخدام مفاتيح من خانتين. وهذا

يزيد عدد المفاتيح الممكنة إلى ١٠٠ (٠-٩٩). وبنفس المعدل السابق سيحتاج المتسلل إلى ١٠٠ ثانية على الأكثر، و٥٠ ثانية في المتوسط، لتخمين المفتاح الصحيح. ولهذا فإن المفاتيح الأطول تُحسِن من الوضع الأمني.

وبما أن أجهزة الحاسب الآلي تقوم بحساب وتدقيق مئات الآلاف من المفاتيح في الثانية، فإن المفاتيح المستخدمة في الواقع العملي تتكون من مئات من الخانات.

الخصائص العامة للخوارزمية:

تشير متطلبات التشفير في الفقرات السابقة إلى بعض الخصائص الهامة لخوارزميات التشفير الجيدة. ويمكن النظر إليها بأنها عملية إدخال المدخلات بطريقة عشوائية. فهيكل المدخلات لـ (النص العادي) عادة يكون في شكل كلمات، صور، وثائق، وغيرها. ولقد رأينا أن المُتسلل إذا تمكن من تخمين أي جزء من الهيكل الداخلي للنص العادي، فإن هذه المعلومات يمكن استغلالها لفك شفرة النص الذي تم تشفيره. ولذلك فإن على خوارزمية التشفير أن تجعل النص المشفر يبدو بأنه تسلسل عشوائي كامل من البتات (bits). لكن يجب أن تكون العملية العشوائية قابلة للاسترداد للمُستخدم الذي يملك المفتاح الصحيح.

وليست رموز الرسالة الفعلية فقط التي يجب أن تبدو عشوائية، بل يجب أيضاً أن يبدو طول النص المشفر عشوائياً للمتسلل. وإذا لم يكن كذلك فإنه في بعض الحالات قد يتمكن المتسلل ببساطة من تخمين محتوى الرسالة من خلال النظر في طول الرسالة والسياق. على سبيل المثال، إذا كانت تعرف في حالة معينة أن هناك خيارين للرسائل: نعم أو لا، وشاهدت الرسالة المشفرة التالية (!$#)، فإنك لا تحتاج إلى فك شفرة الرسالة لأنك ستكون على يقين بأن نص الرسالة (نعم).

وأخيراً، خاصية أخرى مهمة في الخوارزميات هي أن التغيير في بت واحد (bit) من المدخلات يجب أن يقابله تغيير كامل في النص المشفر بما لا يقل عن تغيير نصف البتات (bits). وهذا سوف يمنع المتسلل من محاولة صياغة رسائل انتقائية ومحاولة تخمين نظام التشفير من خلال النظر في مخرجات النص المشفر.

عرفنا في هذه المرحلة أن التشفير ينطوي على خوارزمية ومفتاح. كما عرفنا أن هناك بعضاً من الخوارزميات المستخدمة عالمياً لتشفير المعلومات، وهذه الخوارزميات فريدة من

نوعهـا لكل حالـة، وهذا التميّز يكون من خلال مفتاح فريد لتلـك الحالة. الآن ننتقل إلى أنواع الخوارزميات المستخدمة وتطبيقاتها.

نظرة عامة على أنواع التشفير:

يمكـن تصنيـف جميع تقنيات التشـفير المعروفـة والمتاحة إلى ثلاثة أنـواع حيث يتم التصنيف على أسـاس عدد المفاتيح المسـتخدمة لتشفير وفك تشـفير المعلومات. ويوضح الجدول (٧-١) مقارنة سريعة بين أنواع التشـفير الثلاثة. وما تبقى من هذا الفصل يناقش كل نوع من أنواع التشفير الثلاثة بالتفصيل.

ومن خلال إلقاء نظرة على الجدول نستطيع القول بأن دوال التجزئة (Hash functions) يمكن أن تكون أبسـط أنواع التشفير للفهم. وربما يكون ذلك صحيحاً، لكن عندما يتحدث الناس عن التشـفير عادة ما يقصدون استخدام التشـفير بالمفتاح السري والتشفير بالمفتاح العام. ولذلك سـنناقش في الأقسام التالية أولاً التشفير بالمفتاح السري، وبعد ذلك سنناقش التشـفير بالمفتاح العام. وسـوف نتحدث عن دوال التجزئة في النهاية لأن اسـتخدامها في التشفير أقل شيوعاً من استخدام نوعي التشفير الآخرين.

التشفير بالمفتاح السري (Secret Key Cryptography):

يشير التشـفير بالمفتاح السري إلى طرق التشفير التي تسـتخدم مفتاحاً واحداً لكل من التشفير وفك التشفير. ويقدم الشكل (٧-٣) لمحة عامة عن التشفير بالمفتاح السري.

وكما نرى في الشـكل فإن السـمة الأساسـية في التشـفير بالمفتاح السري هي استخدام المفتاح نفسـه لكل من التشفير وفك التشفير. ونتيجة لهذا التماثل في المفاتيح المستخدمة في التشفير وفك التشفير، تسمى طريقة التشفير بالمفتاح السري «التشفير بالمفتاح المتناظر» (symmetric key cryptography)، أو (symmetric key encryption).

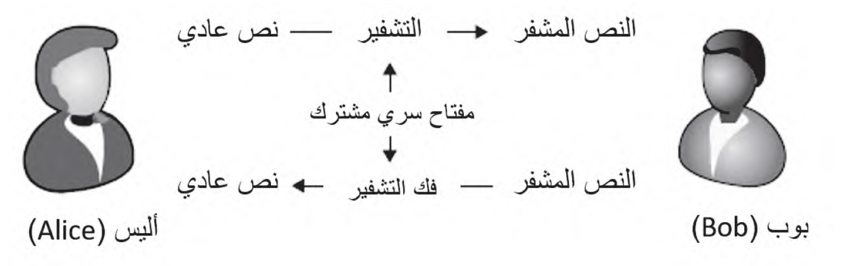
ويسـتخدم (التشـفير بالمفتاح السري) بشكل شائع في نقل المعلومات بشكل آمن. فإذا اتفق كل من أليس (Alice) وبوب (Bob) على استخدام مفتاح موحد، فإن أليس (Alice) تسـتطيع تشـفير معلوماتها بهذا المفتاح كما يسـتطيع بوب (Bob) فك تشفير المعلومات

باستخدام المفتاح نفسه. وبالمثل فإن بإمكان بوب (Bob) تشفير معلوماته بالمفتاح المشترك وبإمكان أليس (Alice) كذلك فك تشفير المعلومات باستخدام المفتاح المشترك نفسه. وستكون المعلومات آمنة أثناء الإرسال لأن أليس (Alice) وبوب (Bob) فقط يعرفان المفتاح، وكما اتفقنا سابقاً، فإنه يكاد يكون من المستحيل فك تشفير المعلومات المرسلة دون معرفة المفتاح.

الجدول (٧-١): مقارنة بين أنوع التشفير

نوع التشفير	المفاتيح	التطبيقات
دوال التجزئة	٠	حماية كلمات المرور، وتدقيق تكامل البيانات
التشفير بالمفتاح السري	١	حفظ ونقل آمن للبيانات
التشفير بالمفتاح العام	٢	ضمان الأمن لكل من تبادل المفاتيح، والمصادقة، والتوقيعات الإلكترونية

الشكل (٧-٣): لمحة عامة عن التشفير بالمفتاح السري



ويمكن أيضاً استخدام (التشفير بالمفتاح السري) لتأمين المعلومات المحفوظة في أجهزة الحاسب الآلي. فإذا أراد بوب (Bob) تأمين بعض المعلومات، عليه اختيار المفتاح ومن ثم تشفير المعلومات المحفوظة في القرص الصلب باستخدام ذلك المفتاح. ولاسترجاع المعلومات، على بوب (Bob) أن يقوم بإدخال المفتاح وفك تشفير المعلومات. وبطبيعة الحال، إذا نسي بوب (Bob) المفتاح فلن يكون قادراً على استرجاع المعلومات المحفوظة في جهاز حاسبه الآلي.

والمعيــار الحالي لـ (التشــفير بالمفتاح السري) هو معيار التشــفير المتقدم (Advanced Encryption Standard). وتــم اختيــار هذا المعيــار من قبل المعهــد الوطني للمعايير والتقنيــة (National Institute for Standards and Technology) في شــهر نوفمبر من عــام ٢٠٠١، وذلــك بعد عملية اختيار اســتمرت ما يقارب من ٥ ســنوات. وقد تم تطوير التقنية المســتخدمة في (معيار التشــفير المتقدم) من قبل اثنين من أخصائيي التشــفير من بلجيكا. ومن التقنيات الســابقة لـ (معيار التشــفير المتقدم) معيار تشفير البيانات (Data Encryption Standard)، وخوارزميــة تشــفير البيانات الدوليــة (International Data Encryption Algorithm)، وهــذان المصطلحــان من المصطلحات التــي قد تواجهها في أدبيــات أمن المعلومات. وبما أن (معيار التشــفير المتقدم) هو المعيــار الحالي المتبع، فلن نناقش (معيار تشــفير البيانات) و(خوارزمية تشفير البيانات الدولية) في الأقسام التالية من هذا الكتاب. وســنقدم في القســم التالي لمحة عن التقنية التي تقف وراء (معيار التشــفير المتقدم).

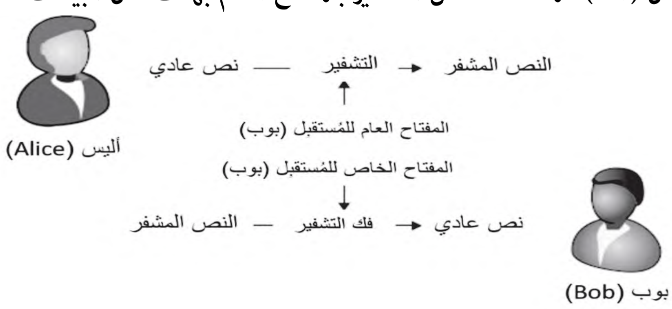
التشفير بالمفتاح العام (Public-key cryptography):

يشــير (التشــفير بالمفتاح العام) إلى طرق التشــفير التي تســتخدم مفتاحين: أحدهما للتشفير والآخر لفك التشفير. وتستخدم هذه التقنية لاثنين من التطبيقات المختلفة - نقل البيانات والتوقيعات الرقمية. ويقدم الشــكل (٧-٤) لمحة عامة عن التشفير بالمفتاح العام بهدف نقل البيانات.

وتُظهر المقارنة بين الشــكل (٧-٣) والشكل (٧-٤) أن الميزة الفريدة لـ (التشفير بالمفتاح العام) هي اســتخدام مفتاح للتشــفير ومفتاح آخر لفك التشفير. وبسبب هذا التفاوت في استخدام المفاتيح فإن (التشفير بالمفتاح العام) يسمى أيضاً «التشفير بالمفتاح غير المتماثل» (asymmetric key cryptography) و(asymmetric key encryption).

وكما سنرى في الأقسام القادمة، وذلك عند مناقشة (التشفير بالمفتاح العام) بمزيد من التفصيل، فإن المفتاح الخاص بالمُستقبِل يظل سرياً. ولهذا السبب فإنه من الشائع الإشارة إلى المفتاح الخاص بالمُستقبِل بأنه المفتاح السري. لكن الباحثين في دراسة (Kaufman et al)[٥] يوصون بتوحيد تسمية هذا المفتاح بـ «المفتاح الخاص» في مجال أمن المعلومات، وتخصيص عبارة «المفتاح السري» للمفتاح السري المشترك والمستخدم في (التشفير بالمفتاح السري). واحتراماً لهذه النصيحة سوف نسعى أيضاً إلى تجنب تسمية المفتاح الخاص بالمفتاح السري.

الشكل (٧-٤): لمحة عامة عن التشفير بالمفتاح العام بهدف نقل البيانات



ما استخدامات التشفير بالمفتاح العام؟ كما سنرى أنه يمكن النظر إلى (التشفير بالمفتاح العام) كإصدار ذي شحنة فائقة من (التشفير بالمفتاح السري). وعلى هذا النحو يمكن لـ (التشفير بالمفتاح العام) ليس فقط القيام بأي عمل يقوم به (التشفير بالمفتاح السري) بل القيام بأكثر من ذلك. إذاً لماذا نهتم بـ (التشفير بالمفتاح السري)؟

تبيّن أن (التشفير بالمفتاح العام) يستنزف الموارد الحاسوبية ويتطلب قدرة معالجة حاسوبية تصل إلى ملايين المرات من تلك المطلوبة لـ (التشفير بالمفتاح السري). وسيؤدي الاستخدام المُفرط لـ (التشفير بالمفتاح العام) بأسرع الأجهزة الحاسوبية المكتبية إلى التوقف شيئاً فشيئاً. ومن ثم فنحن في الواقع العملي انتقائيون للغاية فيما يخص استخدام (التشفير بالمفتاح العام) ونفضل استخدام (التشفير بالمفتاح السري) إلى أقصى حد ممكن.

الاستخدام الرئيسي لـ (التشفير بالمفتاح العـام) هو تبادل المفاتيح. ففي أثناء مناقشة (التشفير بالمفتاح السري) في القسم السابق، هل فكرت في كيفية قيام أليس (Alice) وبوب

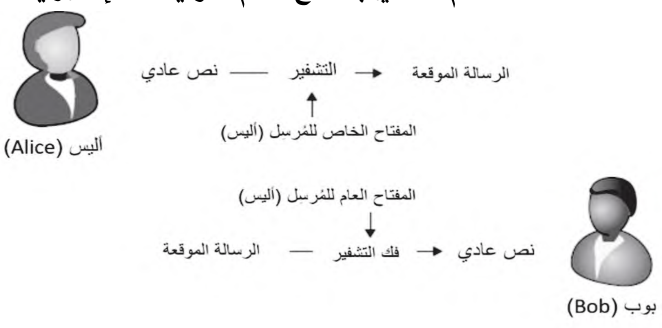
(5) Kaufman, C., R. Perlman and M. Speciner (2002). Network Security: Private Communication in a Public World, Prentice-Hall ISBN 0130460192

(Bob) بالموافقــة على نفس المفتاح السري المشــترك؟ ربما أنــك لاحظت أننا بدأنا بفرضية أن أليــس (Alice) وبــوب (Bob) لديهم مفتاح سري مشــترك. وذلك قد يكــون ممكناً إذا كان أليــس (Alice) وبــوب (Bob) في مكاتب متجاورة. ولكن ما هو الوضع إذا كان بوب (Bob) يُمثل مزود الخدمة الموجود في مدينة واشــنطن العاصمة، وكانت أليس (Alice) تُمثل العميل الموجــود في مدينة تامبا في ولاية فلوريدا؟ هل هناك وســيلة لأليــس (Alice) وبوب (Bob) للاتفاق على مفتاح سري مشترك دون أن يعرفه أحد؟ الإجابة كلا. وفي الواقع يمكن إثبات أنه لا يوجد طريقة يمكن الاعتماد عليها لأليس (Alice) وبوب (Bob) لتبادل مفتاح سري آمن(٦) .

ولأنه ليس هناك وســيلة عاديــة لأليس (Alice) وبوب (Bob) لتبــادل المفتاح السري بشــكل آمن، فإن (التشــفير بالمفتاح العام) يســتخدم للقيام بهذه المهمة. وعندما يكون أليــس (Alice) وبوب (Bob) على اســتعداد للتواصل معاً، فإنهم يســتخدمون (التشــفير بالمفتاح العام) لتبادل المفتاح السري. وعندما يتم الاتفاق على المفتاح السري، يتحول أليس (Alice) وبوب (Bob) من استخدام (التشفير بالمفتاح العام) المُستنزِف للموارد الحاسوبية إلى استخدام (التشفير بالمفتاح السري) الأبسط والأقل استنزافاً للموارد الحاسوبية.

من المهم أن نتذكر هذه النقطة حول (التشفير بالمفتاح العام) - صاحب المفتاح هو الوحيد الذي يعرف المفتاح الخاص، ولا يتم مشاركته مع أي شخص آخر.

الشكل (٧-٥): استخدام التشفير بالمفتاح العام للتوقيعات الإلكترونية



(٦) في الأدبيات تمت مناقشة هذا السيناريو على أساس مشكلتين عامتين. وهناك الكثير من المعلومات المتوفرة حول هذه المشكلة المعروفة على شبكة الإنترنت. انظر على سبيل المثال المقال التالي موقع ويكيبيديا،
http://en.wikipedia.org/wiki/Two_Generals%27_Problem

أما الاســتخدام الثاني لـ (التشــفير بالمفتاح العام) تأتي من العلاقــة الفريدة بين المفتاح العــام والمفتــاح الخاص المرتبط بــه حيث تبيّن أن تلك المفاتيح توجــد في أزواج. لقد رأينا أن المعلومات المشــفرة باســتخدام المفتاح العام يمكن فك تشفيرها بواسطة المفتاح الخاص المرتبــط بذلك المفتــاح العام. ويمكن لهــذه العملية أن تعمل أيضــاً في الاتجاه المعاكس. المعلومات المشــفرة باســتخدام المفتاح الخاص يمكن فك تشــفيرها بواســطة المفتاح العام المرتبط بذلك المفتاح الخاص. ويتم اســتخدام هذه الميزة في مجال أمن المعلومات لإنشــاء التوقيعات الرقمية. وتعرف التوقيعات الرقمية بأنها تحويلات مشــفرة من البيانات تسمح لمُستقبِل البيانات بإثبات مصدر البيانات (عدم التنصل) وتكاملها.

عندما تُرســل أليس (Alice) رســالة إلى بوب (Bob) فإنه يمكنها أيضاً أن ترســل نسخة مشفرة من الرسالة تتضمن المفتاح الخاص بها. وبإمكان بوب (Bob) أن يحاول فك شفرة المعلومات. وإذا كانت النســخة التي تم فك شــفرتها توافق المعلومات المُرســلة فإن بوب (Bob) على يقين بأن أليس (Alice) هي التي أرسلت المعلومات وأن الرسالة لم يتم تعديلها وهي في طريق الإرسال. وتظهر هذه العملية في الشكل (٧-٥).

ويمكن أن يكون (التشــفير بالمفتاح العام) محيراً للقارئ الذي يقرأ عنه لأول مرة. ومن المربــك أيضاً أن نرى اســتخدامَين مختلفَين لهذه التقنية المحيرة. ولتســهيل التعلم في هذا الفصل سنتبع خطوتين مختلفين: الخطوة الأولى هي مقارنة الشكلين (٧-٤) و(٧-٥) وتحديد الفروقات الموجودة بينهما. أما الخطوة الثانية فســتكون في القســم التالي من خلال شرح (التشفير بالمفتاح العام) باستخدام مثال.

دعنا ننظر إلى الشكلين (٧-٤) و(٧-٥).

ما المفاتيح المستخدمة في كل حالة؟ لنقل البيانات استخدمنا مفاتيح المُستقبِل. وللتوقيعات الرقمية استخدمنا مفاتيح المُرسِل. ولنقل البيانات استخدمنا المفتاح العام للتشفير. وللتوقيعات الرقمية استخدمنا المفتاح الخاص للتشفير، والجدول (٧-٢) يُلخص ذلك.

ما الذي يحدث هنا؟ لماذا الاختلاف في المفاتيح المستخدمة؟ الشيء الضروري الذي يجب أن نتذكره بخصوص (التشــفير بالمفتاح العام) أن المســتخدم يمكنه الوصول إلى مفتاح خاص واحد وهو المفتاح الذي يملكه. لكن الجميع لديه حق الوصول إلى جميع المفاتيح العامة.

الجدول (٧-٢): مقارنة لتطبيقات التشفير بالمفتاح العام

	نقل البيانات	التوقيع الرقمي
مالك المفتاح	المُستقبِل	المُرسِل
نوع مفتاح التشفير	عام	خاص

وعنـد نقل البيانـات، نرغب في التأكد مـن أن تلك البيانات لا يمكـن قراءتها من قبل الآخرين أثناء الإرسال. وأفضل طريقة لتحقيق ذلك هي تشفير المعلومات بطريقة يستطيع المُسـتقبِل فقط من خلالها فك شفرة المعلومات. كيف نفعل ذلك؟ وما الشي الفريد لدى المُستقبِل؟

حسناً نحن نعلم أن المُستقبِل يملك فقط المفتاح الخاص به. كما نعلم أيضاً أننا إذا قمنا بتشـفير بعض المعلومات باستخدام المفتاح العام للمُسـتقبِل، فإن المُستقبِل فقط سيكون قادراً على فك شفرة المعلومات باستخدام مفتاحه الخاص. ولحسن الحظ فإن أي شخص في العالم يمكنه الحصول على المفتاح العام لأي مسـتخدم. لذلك هذا ما سوف نفعله - تشفير المعلومات باسـتخدام المفتاح العام للمُستقبِل ومن ثم إرسالها. وعندها سيكون المُستقبِل فقط قادراً على قراءة المعلومات.

عند التوقيع على الرسائل فإن الخصوصية ليست مصدراً للقلق. على سبيل المثال، يرغب بوب (Bob) أن يكون مقتنعاً بأن أليس (Alice) هي بالفعل من قامت بإرسـال الرسالة[٧]. كيف يمكن لأليس (Alice) القيام بذلك؟ حسناً، كلٌّ من أليس (Alice) وبوب (Bob) يعلم أن فقط أليس (Alice) تملك المفتاح الخاص بها. إذا كانت أليس (Alice) تسـتطيع إقناع بـوب (Bob) بطريقة أو بأخرى بأنها بالفعل تمتلك هذا المفتاح، فإن بوب (Bob) سـوف يقتنع. ولحسـن الحظ لدينا طريقة للقيام بذلك. إذا قامت أليس (Alice) بتشـفير بعض المعلومات باستخدام مفتاحها الخاص، فإن أي شخص في العالم يستطيع فك شفرة المعلومات باستخدام مفتاحها العام. وفي الواقع فإن بوب (Bob) يقوم بذلك بالضبط. وإذا نجح فإنه

---

(٧) افترض أنك تلقيت عرضاً للعمل من البيت الأبيض بدون دعوة سابقة. كيف يمكنك أن تكون على قناعة بأن ذلك العرض حقيقي؟

سيكون مقتنعاً بأن أليس (Alice) تملك المفتاح الخاص الذي يُفترض أن يكون لديها. ولأنه لا أحد في العالم يجب أن يكون لديه المفتاح الخاص بأليس (Alice)، فإن الرســالة يجب أن تكون أُرسلت من أليس (Alice). ومن ثم فإن المفتاح العام يعمل بمثابة توقيع رقمي.

الطريقة التي يتم بها استخدام التوقيعات الرقمية في الواقع العملي تعطي ميزة إضافية. ما الرســالة التي يجب أن تقوم أليس (Alice) بتشــفيرها وإرسالها إلى بوب (Bob) لإقناعه بهويتها؟ نحن نقوم بتشــفير الرســالة، وبهذه الطريقة إذا اســتطاع بوب (Bob) أن يفك الشفرة بنجاح سيقتنع بأن الرسالة ليست فقط أرسلت من أليس (Alice)، بل سيتأكد أيضاً أن الرسالة لم يعدَّل عليها في أثناء الإرسال.

> لقد تم تبسيط النقاش أعلاه بالمقارنة مع ما يحدث في الواقع. وقد تم ذلك التبسيط لأغراض تعليمية. وفي الواقع العملي لسنا بحاجة لتشفير الرسالة بالكامل. نحن بحاجة فقط لتشفير دالة التجزئة (hash function) الخاصة بالرسالة. وسنناقش دوال التجزئة في القسم التالي، كما سنعيد النظر في هذا الموضوع في نهاية مناقشة دوال التجزئة.
>
> ويمكن أنك فكرت في السؤال التالي: كيف يمكن لأليس (Alice) الحفاظ على سرية الرسالة خلال إرسال البيانات إذا كان أي شخص يستطيع فك شفرة الرسالة باستخدام المفتاح العام الخاص بأليس (Alice)؟ سؤال رائع. لا تستطيع أليس (Alice) القيام بذلك. ومن ثم فإن ما نقوم به هو إرسال الرسالة باستخدام تقنية إرسال البيانات التي تم نقاشها أعلاه، ونُرسل أيضاً توقيع رقمي جنباً إلى جنب مع الرسالة لتأكيد أن الرسالة أُرسلت بالفعل من أليس (Alice).

وتُسمى التقنية الحالية المستخدمة لتنفيذ (التشفير بالمفتاح العام) بـ (RSA). وسُميت هذه التقنية بأســماء العلماء الثلاثة الذين أنشؤوا هذه التقنية وهم: رون ريفست (Ron Rivest)، وآدي شــمير (Adi Shamir)، وليونــارد أديلــمان (Leonard Adleman). وتم شرح هذه التقنية في دراسة نُشرت في عام ١٩٧٧ [٨].

(8) Rivest, R. Shamir, A. and Adleman, L. «A method for obtaining digital signatures and public-key cryptosystems.» Communications of the ACM, 1978, 21(2): 120–126. (The first few pages of the paper should be very interesting for an undergraduate student – the opening line talks about email in future tense.) The paper is also available at http://people.csail.mit.edu/rivest/Rsapaper.pdf (accessed: 10/19/2012).

دوال التجزئة (Hash functions):

تشـير دوال التجزئة إلى طرق التشـفير التي لا تسـتخدم مفاتيح. وتسمى هذه الدوال أيضاً تحولات الاتجاه الواحد (one-way transformations) لأنه لا توجد وسيلة لاسترداد الرسـالة المشفرة باسـتخدام دالة التجزئة. وهذا يجعل القارئ يُبدي علامات الحيرة. لماذا نهتم بتقنية تشفير إذا كانت لا تسمح أبداً بقراءة البيانات مرة أخرى؟ كما اتضح أن هذه التقنيـة في الواقع مفيدة جداً وأنك في الحقيقية تسـتخدم هذه الخاصية منذ اسـتخدامك لأجهزة الحاسب الآلي.

دوال التجزئة تأخذ الرسائل مهما كان طولها وتقوم بتحويلها إلى أرقام ذات طول ثابت، ويكـون طولها عادة ١٢٨ أو ٢٥٦ بت (bit). فعند التحويل يكون طول دالة التجزئة للرقم (٤) هو نفسـه طول دالة التجزئة لبيانات القرص المتعدد الاسـتخدامات الرقمي (DVD) كاملاً. وتُستخدم دوال التجزئة مع كلمات المرور، وسنرى كيف يكون ذلك في الفقرة التالية، وفي الوقت الحالي قد يكون تمريناً مناسباً لك أن تفكر كيف تكون دوال التجزئة مفيدة مع كلمات المرور.

تحتفظ أجهزة الحاسب الآلي بكلمات المرور نتيجة لتحويل دوال التجزئة بدلاً من حفظ القيم الحقيقية لكلمات المرور. وبهذه الطريقة لا يمكن استرداد كلمات المرور حتى في حال سرقة جهاز الحاسـب الآلي. فعندما يقوم المسـتخدم بإدخال كلمة المرور الخاصة به، فإن جهاز الحاسب الآلي يحسب دالة التجزئة لكلمة المرور ويقارنها مع دالة التجزئة المحفوظة في جهاز الحاسـب الآلي. وإذا تطابقت الاثنتان فإن جهاز الحاسـب الآلي يقبل كلمة المرور المدخلة وإلا فإنه يرفضها. وبهذه الطريقة فإن دوال التجزئة تسـمح لأجهزة الحاسب الآلي بالتحقق من كلمات المرور دون حفظ نسخة من كلمات المرور نفسها.

> كلمات سر دوال التجزئة لا تزال عرضة لهجمات القوة الغاشمة (brute-force attack) وهجمات القاموس (dictionary attack) كما سنرى ذلك في الفصل الثامن. فإذا اختار المستخدم كلمة مرور ضعيفة، فإنه من الممكن تخمينها بسهولة. وتقوم دوال التجزئة بحجب كلمات المرور لكنها لا يمكن أن تمنع أحداً من أن يقوم بتخمين كلمات المرور تلك.

والاســتخدام الآخر لكلمات المرور هو التحقق من تكامل المعلومات. فإذا أرسل المُرسِل الرســالة وأرسل أيضاً دالة التجزئة، يستطيع المُســتقبِل بشكل مستقل حساب دالة التجزئة للرســالة ومقارنتها بدالة التجزئة المُســتلمَة. وعند تطابق الدالتين فإن المُستقبِل يتأكد من أن الرســالة لم يتم تعديلها أثناء الإرســال. وعند استخدام دوال التجزئة بهذه الطريقة فإنه يُطلــق عليها خاصية المجموع الاختيــاري (checksums). والمجموع الاختياري هو قيمة يتم حسابها بناء على البيانات بهدف كشف الأخطاء أو كشف التلاعب في البيانات في أثناء الإرسال.

ونــرى هذا عادة أثناء تحميل البيانات حيــث يوفر موردي البرمجيات خاصية المجموع الاختياري لتحميل برمجياتهم بهدف مســاعدة مسؤولي النظم على التحقق من أن البرنامج تم تحميله دون أخطاء. ويوضح الشــكل (٧-٦) مثالاً من موقع التحميل لخوادم تطبيقات شركة آي بي إم (IBM Application Servers).

الشكل (٧-٦): مثال على خاصية المجموع الاختياري

publib.boulder.ibm.com/wasce/md5/3002/wasce-3.0.0.2.md5

```
e5943edf209b9da610c353cb0795521d *wasce_ibm60sdk_setup-3.0.0.2-390xlinux.tar.bz2
7b6f822fd58983bd0c515d9367f3d96b *wasce_ibm60sdk_setup-3.0.0.2-ia32linux.tar.bz2
11fe3732c4fd5b36ebb9d88a79f29e4d *wasce_ibm60sdk_setup-3.0.0.2-ia32win.zip
f0bfa0992320afe1f77a43abda82695f *wasce_ibm60sdk_setup-3.0.0.2-ppc64aix.zip
bed57127a2a5a2560665158e18658c86 *wasce_ibm60sdk_setup-3.0.0.2-ppc64linux.tar.bz2
9fa2d5850312698a4807b0f0b4a10135 *wasce_ibm60sdk_setup-3.0.0.2-sparc64solaris.zip
4ddaa95fac2756a0ab86a3325193a2de *wasce_ibm60sdk_setup-3.0.0.2-x86_64linux.tar.bz2
4d9d9837939194119f04f8e4cd35e2b4 *wasce_ibm60sdk_setup-3.0.0.2-x86_64win.zip
69baf09b42e4fbcb495820b496502998 *wasce_ibm70sdk_setup-3.0.0.2-390xlinux.tar.bz2
137f9df15928884be80110279448b1ba *wasce_ibm70sdk_setup-3.0.0.2-ia32linux.tar.bz2
afe7679f636f64cafd6a980ffc0a10a5 *wasce_ibm70sdk_setup-3.0.0.2-ia32win.zip
a6ac0247a621021f4dcc24b77e5cbf6f *wasce_ibm70sdk_setup-3.0.0.2-ppc64aix.zip
0ab7e54a940c95b2d16c92e7e5f20620 *wasce_ibm70sdk_setup-3.0.0.2-ppc64linux.tar.bz2
3e3f5bdb678000fba9190e955c9dc092 *wasce_ibm70sdk_setup-3.0.0.2-sparc64solaris.zip
cf2412a7522ce2c805a080ae7c547c5c *wasce_ibm70sdk_setup-3.0.0.2-x86_64linux.tar.bz2
bf01e274304c8abe2be1568c75bd0f2e *wasce_ibm70sdk_setup-3.0.0.2-x86_64win.zip
b2791cf15dd7f97370783fcbc88c8cd9 *wasce_samples-3.0.0.2.zip
ac591620e85bd9be8acf64c2443e6658 *wasce_setup-3.0.0.2-unix.bin
c359de0e70fce73fd1f2fa3cd65f5113 *wasce_setup-3.0.0.2-win.exe
```

ودوال التجزئة الأكثر استخداماً وشيوعاً هما دالة (MD٥) ودالة (SHA-٢). وتمثل دالة (MD٥) «خوارزميات خلاصة الرسالة» (message digest algorithms). وقد استُخدمت هذه الدالة عالمياً منذ تطويرها في عام ١٩٩١من قبل رون ريفســت (Ron Rivest) (وهو نفســه الذي شــارك في تطوير بروتوكول RSA). لكن تم اكتشاف مجموعة من العيوب في الخوارزمية، ومن ثم فإن اســتخدامها في تطبيقات التشــفير لم يلق تشجيعاً رسمياً منذ ٣١

ديســمبر من عام ٢٠٠٨ [٩]. ومع ذلك لا تزال هذه الدالة شــائعة الاستخدام في التطبيقات المنخفضة المخاطر مثل التحقق من تحميل البرمجيات.

أمــا دالــة (SHA-٢) فهي تمثــل «خوارزميــة دالة التجزئــة الآمنــة» (secure hash algorithm)، ويرمــز الرقــم (٢) إلى الإصدار الثاني من الخوارزميــة. وقد تم تطوير هذه الخوارزمية من قبل المعهد الوطني للمعايير والتقنية (National Institute of Standards and Technology)، وتــم إصدارهــا في عــام ٢٠٠١. وعلى الرغم من عــدم وجود ثغرات أمنيــة معروفة لهذه الخوارزمية إلا أن الإصدار التالي لهــذه الدالة (SHA-٣) كان في الثاني مــن أكتوبر من عام ٢٠١٢[١٠]. وكان الدافع لتطويــر الجيل التالي لدالة التجزئة قبل وجود حاجة واضحة لذلك هو البقاء على اســتعداد في حــال حدوث هجوم ضد دالة (SHA-٢). وتستخدم دالة (SHA-٣) خوارزمية مختلفة تماماً مقارنة بـ (SHA-٢) لذلك فمن المستبعد جــداً أن الهجــوم الذي يخترق دالــة (SHA-٢) أن يكون قادراً على اخــتراق دالة (SHA-٣). ولدى المطورين الآن الخيار في اســتخدام دالــة (SHA-٢) أو دالة (SHA-٣) بناءً على احتياجاتهم.

تفاصيل أنواع التشفير:

قدّم القسم السابق لمحة عامة عن أنواع التشفير الثلاثة واستخداماتها. وفي هذا القسم سننظر بمزيد من التفصيل في التقنيات الأولية المستخدمة في كل نوع من أنواع التشفير.

التشفير بالمفتاح السري (Secret Key Cryptography):

يتكــون التشــفير بالمفتاح السري من إجراءين: تشــفير المجموعات وتسلســل تشــفير المجموعات. ويتطلب تشــفير الرســائل الكبــيرة ذات الحجم غير المحدد موارد حاســوبية هائلــة تفوق قدرات معظم أجهزة الحاســب الآلي للمســتخدم النهائي، ومــن ثم يتم أولاً تقسيم بيانات المستخدم إلى مجموعات ذات حجم ثابت بحيث يمكن إدارتها. ويتم تقسيم الرســائل إلى أحجام معقولة تمنح مزيجاً من الأداء والأمان. ويُنظر إلى تشــفير المجموعات

(9) http://www.kb.cert.org/vuls/id/836068

(10) http://csrc.nist.gov/groups/ST/hash/sha-3/index.html

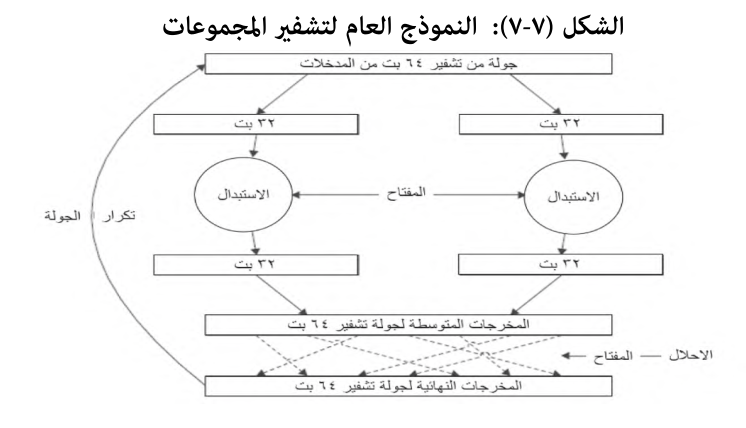
بأنــه عملية تحويل مجموعات النص العادي إلى مجموعات مشــفرة. ومعظم خوارزميات التشــفير التجارية تســتخدم مجموعات ٦٤ أو ١٢٨ بت (bit). وعلى وجه الخصوص فإن المعيار الحالي لتشفير المفتاح السري (AES) يستخدم مجموعات ١٢٨ بت (bit).

تشفير المجموعات (Block Encryption):

بشــكل عام يســتخدم تشــفير المجموعات مزيجاً من النشــاطين التاليين: الاســتبدال والإحلال. لقد رأينا مثالاً على (الاســتبدال) ســابقاً في هذا الفصل: شفرة قيصر والاستبدال الأحادي الأبجدي (mono-alphabetic substitution). وفي سياق التشفير بالمفتاح السري، يحدد (الاســتبدال) مخرجــات ١٠٠٠ بت (k-bit) لكل ١٠٠٠ بــت (k-bit) من المدخلات. أمــا (الإحلال) فيحــدد مكان المخرجات لــكل ١٠٠٠ بت من المدخــلات. ويعد (الإحلال) حالة خاصة من الاســتبدال لأن كل بت (bit) من المدخلات تَســتبدِل بت (bit) محدد من المخرجات. ويوضح الشكل (٧-٧)[11] العملية العامة لتشفير المجموعات.

ويمثل الشــكل (٧-٧)، والمســتند إلى تقنية معيار تشفير البيانات (DES technology)، العمليــة العامــة لتقنيات التشــفير بالمفتاح السري حيث يتم داخل كل مجموعة تقســيم البيانات إلى قسمين. ويقوم إجراء (الاستبدال) بضغط جميع البتات (bits) في كلا القسمين. ويتم تمرير كلا القســمين المضغوطين على وحدة الإحــلال والتي تقوم بخلط جميع البتات (bits) في المجموعة. وتتكرر هذه العملية حتى يتم تشفير المدخلات بشكل مُرضٍ.

الشكل (٧-٧): النموذج العام لتشفير المجموعات



(11) تم اقتباس الصورة من: FIPS PUB 46-3, 10 Data Encryption Standard (DES), 25/99., http://csrc.nist. gov/publications/fips/fips46-3/fips46-3.pdf, (accessed 10/23/12).

لماذا الإحلال؟

قد يسأل قارئ مهتم السؤال التالي: إذا كان (الإحلال) شكلاً خاصاً من (الاستبدال) فقط، لماذا نستخدمه من الأساس؟ لماذا لا نكرر عمليات (الاستبدال) عوضاً عن (الإحلال)؟

السبب وراء استخدام (الإحلال)هو نشر تأثير (الاستبدال) إلى أبعد حد. إذا نظرت في الشكل (٧-٧) بتأمل ستجد أنه إذا تغيرت بت واحدة (bit) في النصف الأيسر من المدخلات، فإن عملية (الاستبدال) تؤثر فقط في البتات (bits) في النصف الأيسر من المخرجات. وينطبق الشيء نفسه على تغيير البتات في النصف الأيمن من المدخلات - عملية (الاستبدال) تؤثر فقط في البتات في النصف الأيمن. وبإمكان الشخص المُخرب استخدام هذه الخاصية لصياغة مدخلات خاصة ومن ثم اختراق خوارزمية التشفير. لذا فإن عملية (الإحلال) تنشر تأثير التغيير في بت واحدة إلى المخرجات الإجمالية للمجموعة.

يتم تكرار عملية الاســتبدال - الإحلال عدة مرات لضمان أن التغييرات في المدخلات تم توزيعها على جميع البتات (bits) في المخرجات. وفي الشــكل (٧-٧)، ســيؤثر التغيير في بت واحــدة من المدخلات على ٣٢ بتاً من ٦٤ بتــاً في المخرجات في الجولة الواحدة (إما النصف الأيمــن أو النصف الأيسر، يليها تغييرات في ٣٢ بتاً المُقابلــة من المخرجات الأخيرة للجولة). وهذا ليس مُرضياً. فللحصول على تشــفير جيد، يجب أن يؤثر أي تغيير في بت واحدة من المدخلات على جميع الـ ٦٤ بتاً في المخرجات على حد سواء. وهذا سيجعل التشفير صعب الاختراق على المتســلل. ولتحقيق ذلك يتم تكرار الجولات حتى تتأثر جميع البتات (bits) بأي تغيير في المدخلات حتى لو كان بســيطاً. معيار تشــفير البيانات (DES) يســتخدم ١٦ جولة. ومعيار التشفير المتقدم (AES) يستخدم ١٠-١٤ جولة اعتماداً على حجم المفتاح.

الخلط- النشر:

تسلسل الاستبدال - الإحلال لخوارزمية تشفير المجموعة يُحقق أفكار «كلود شانون» (Claude Shannon) عن الخلط والنشر. شانون، والذي يُعد على نطاق واسع والد نظرية المعلومات، وضع فكرة أن الخلط والنشر يوفران أساساً جيداً لسريّة الأنظمة[١٢]. الخلط هو جعل العلاقة بين النص العادي والنص المشفر معقدة قدر الإمكان. أما النشر فهو توزيع تأثير التغيير في بت واحدة من النص العادي على جميع البتات (bits) في النص المشفر.

في تشفير المجموعة، الاستبدال يوفر الخلط في حين أن الإحلال يوفر النشر.

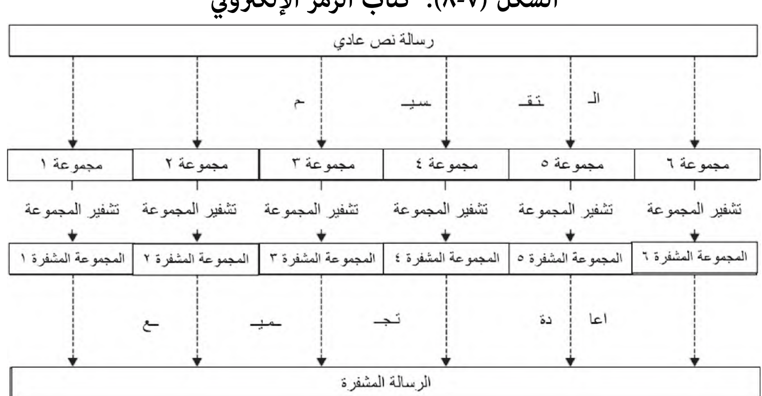
تسلسل تشفير المجموعات (Cipher block chaining):

عندما يتم تشــفير المعلومات الموجودة في المجموعة، نحتاج إلى وســيلة لاستخدام هذه

(12) Shannon, C. «Communication theory of secrecy systems,» 1946,http://netlab.cs.ucla.edu/wiki/files/shannon1949.pdf (accessed 10/23/12).

الآلية لتشــفير الحجم العشــوائي للمعلومات. والفكرة الأساسية وراء الطرق المستخدمة في الواقع العملي لتحقيق هذا الهدف هي جمع كل المجموعات المشفرة وتجميعها معاً بشكل مناسب للحصول على نسخة مشفرة لإدخالات المستخدم. والطريقة الأساسية لتحقيق ذلك قد تكون مجرد جمع المجموعات كما هو مبين في الشكل (٧-٨). وهذه الطريقة سهلة جداً للفهم لكنها غير مستخدمة في الواقع العملي لأسباب سنذكرها بعد قليل. لكن نظراً للأهمية النظرية لهذه الطريقة، أُعطيت هذه الطريقة اســم «كتاب الرمز الإلكتروني» (electronic code book). وكتاب الرمز الإلكتروني هو عملية تقســيم الرسالة إلى مجموعات، ومن ثم تشفير كل مجموعة على حدة.

الشكل (٧-٨): كتاب الرمز الإلكتروني



لماذا لا يتم اســتخدام (كتاب الرمز الإلكتروني) في الواقع العملي؟ الشــكل (٧-٨) يوضح أن هناك انتشــاراً غير كافٍ للخلط في هذه الطريقة. إذا كانت المجموعة الأولى والمجموعة الثالثــة متطابقتــين، فإن المجموعة المشــفرة الأولى والمجموعة المشــفرة الثالثة ســتكونان متطابقتين أيضاً، وهذا سيكون واضحاً في المخرجات المشفرة النهائية. وهذا يمكن أن يعطي المهاجــم لمحة عن المعلومات التي تم تشــفيرها. لذلك لا بد مــن إدخال بعض التعقيد في الواقع العملي لنشر المخرجات بشكل كاف. ومن هذه الطرق، والتي يمكن فهمها بسهولة، طريقة تُدعى تسلســل تشــفير المجموعات (cipher block chaining) والتي تســتخدم معلومات من المجموعة المشفرة السابقة أثناء تشفير مجموعة ما. وهذا الآلية موضحة في الشكل (٧-٩).

الفرق بين (كتاب الرمز الإلكتروني) و(تسلســل تشــفير المجموعات) هو أنه قبل تشفير مجموعة ما، يتم ضغط تلك المجموعة بمخرجات من المجموعة الســابقة. وتوضح الأســهم القطرية في الشــكل أن المخرجات المشــفرة للمجموعة الســابقة يتم اســتخدامها لضغط مدخــلات المجموعــة التاليــة. والعملية المســتخدمة عــادة للدمج بين المُدخلَين تســمى (exclusive OR)، وتكتب هكذا (XOR)، وهي ممثلة في الشكل (٧-٩) بعلامة الزائد (+). وتقوم عملية (XOR) بمعالجة البت حيث تكون النتيجة (٠) إذا كانت قيمة البت لكلٍ من المُدخلَين متســاوية، أو تكون النتيجة (١) إذا كانت قيمة البت لكلٍ من المُدخلَين مختلفة. ونتيجة لتسلســل المُخرجات فإن المجموعة المشــفرة الأولى والمجموعة المشــفرة الثالثة لن تكونا متطابقتين وإن كانت المجموعة الأولى والمجموعة الثالثة متطابقتين.

يتم اختيار (ناقل التهيئة) عشــوائياً للعمل على ضمان أنه إذا تم إرســال الرسالة نفسها مرة أخرى فإن المخرجات ســتكون مختلفة تماماً. وببســاطة يتــم الحصول على المخرجات النهائية لـ (تسلسل تشفير المجموعات) عن طريق تجميع المجموعات المشفرة معاً كما هو موضح في الجزء السفلي من الشكل (٧-٩).

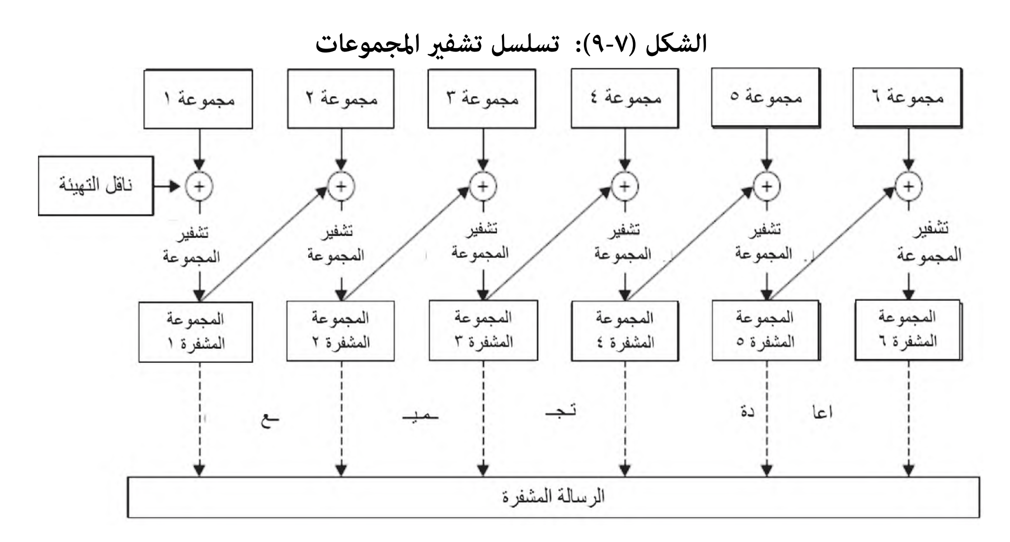
وكما يتضح من هذا القسم يعتمد (التشفير بالمفتاح السري) يعتمد على عمليات بسيطة إلى حد ما، لذلك يُعد (التشــفير بالمفتاح السري) طريقة مُتحفظة حسابياً للغاية. لكن كما ناقشــنا سابقاً في هذا الفصل يمكن التحدي في استخدام (التشفير بالمفتاح السري) يكمن في تبادل المفاتيح حيث يجب أن يكون كل من المُرسل والمُستقبل قادراً على تبادل المفتاح قبل الشروع في عملية التشفير. (التشفير بالمفتاح العام)، والذي سنناقشه في القسم التالي، يحقق هذا الهدف. وعلى الرغم من أن (التشفير بالمفتاح العام) يستنزف الموارد الحاسوبية للجهاز إلا أن أكــبر ميزة له هي إتاحة التواصل السري عــبر القنوات غير الآمنة. ولذلك يعد مثالياً للاستخدام في تبادل المفاتيح.

التشفير بالمفتاح العام (Public-key cryptography):

يستخدم (التشفير بالمفتاح العام) مفتاحين: الأول للتشفير والآخر لفك التشفير. ويوزَّع مفتاح التشــفير على نطاق واسع للسماح للمستخدمين بإرسال رسائل مشفرة لمالك المفتاح.

أما مفتاح فك التشفير فيُستخدم لفك التشفير، ومن الواضح أن صاحب المفتاح يحافظ على مفتاحه بعناية. ولهذا السـبب فإن مفتاح التشـفير يُسمى المفتاح العام، في حين أن مفتاح فك التشفير يُسمى بالمفتاح الخاص. وللحفاظ على النقاش مختصراً ومبسطاً قدر الإمكان في هذا القسم، سـنقدم مثالاً مُبسطاً للحساب المعياري (modular arithmetic) الذي يقف وراء أكثر خوارزميات (التشـفير بالمفتاح العام). بعد ذلك نسـتعرض خوارزمية (التشـفير بالمفتاح العام) الأكثر شيوعاً وهي خوارزمية (RSA).

الشكل (٧-٩): تسلسل تشفير المجموعات



الحساب المعياري (modular arithmetic) المُستخدم في (التشفير بالمفتاح العام):

أحيانـاً يُطلق عـلى عمليـة المُعامِـل (modulus operation) عملية باقي القسـمة (remainder). لذا فإن:

(94 mod 10 = 4 17)، (mod 10 = 7)، وهكذا.

ويوضح الجدول (٧-٣)[١٣] عملية اسـتخدام معامل باقي القسـمة في التشـفير بالمفتاح العام. ويوضح الجدول كيف تتم عملية تشفير الأرقام العشرية.

---

(١٣) هذا الجدول يعتمد على المثال الموجود في الدراسة التالية (Kaufman, C. Perlman. R. and Speciner, M. 2002. Network Security: Private Communication in a Public World. Prentice-Hall)

ولاســتخدام جدول تشفير البيانات، تُضرب الأعداد الموجودة في رأس الجدول في ٣ ومن ثم يجري اســتخدام معامل باقي القســمة على ١٠. على ســبيل المثال، لتشفير العدد (٦)، نضرب ٦ في ٣ ونحسب معامل باقي القسمة على ١٠ كما يلي:

(6*3 mod 10 = 18 mod 10 = 8).

ومن ثم فإن العدد (٨) هو النص المشــفر للعــدد (٦). ويوضح الصف الأول المظلل في هذا الجدول النص المشفر المحسوب بهذه الطريقة لجميع الأرقام ذات الخانة الواحدة.

ولفك التشــفير نضرب النص المشــفر في ٧ ونحسب معامل باقي القسمة على ١٠. على سبيل المثال،

(8*7 mod 10 = 56 mod 10 = 6).

لاحظ أن النتيجة تســاوي ٦ والتي تم تشفيرها سابقاً إلى ٨. وفي الجدول تلاحظ النتائج لجميع الأرقام الأخرى في الصف الثاني المظلل من الجدول.

وفي هــذا المثــال يمكننا كتابة (٣، ١٠) على أنها مفتاح التشــفير (العام)، و (٧، ١٠) على أنها مفتاح فك التشــفير (الخاص). وفي هذا المثال هناك حقيقتان مثيرتان للاهتمام تتعلق باستخدام معامل باقي القسمة:

أولاً، البيانات المشــفرة باستخدام مفتاح التشفير لا يمكن فك تشفيرها باستخدام مفتاح التشفير. على سبيل المثال،

(8*3 mod 10 = 24 mod 10 = 4).

وبمــا أن العــدد (٤) لا يســاوي العدد (٦) فإنه لا يمكن للمتســلل أن يســتغل معرفته بالمفتــاح العام لفك شــفرة البيانات المشــفرة بنفس المفتاح. ومن ثم فــإن معرفة المفتاح الخاص ضرورية لفك التشفير.

ثانياً، بالإمكان استخدام أي من المفتاحين في التشفير ومن ثم فإن المفتاح الآخر سيعمل مفتاحاً لفك التشفير. على سبيل المثال، (٦*٧ mod ١٠ = ٢) (تشفير)، و (٢*٣ mod ١٠ = ٦) (فك التشــفير). وهذا يسمح لاستخدام (التشفير بالمفتاح العام) في التوقيعات الرقمية كما ذكرنا سابقاً في هذا الفصل.

الجدول (٧-٣): جدول معامل القسمة على ١٠ لتوضيح أساسيات التشفير بالمفتاح العام.

الرقم المطلوب تشفيره (n) ← (نص عادي)		٠	١	٢	٣	٤	٥	٦	٧	٨	٩
المفتاح (المضاعف) (m)	↓										
	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠	٠
(n)*(m) mod ١٠ ←	١	٠	١	٢	٣	٤	٥	٦	٧	٨	٩
(n)*(m) mod ١٠ ←	٢	٠	٢	٤	٦	٨	٠	٢	٤	٦	٨
(n)*(٣) mod ١٠= النص المشفر (c) ←	٣	٠	٣	٦	٩	٢	٥	٨	١	٤	٧
	٤	٠	٤	٨	٢	٦	٠	٤	٨	٢	٦
	٥	٠	٥	٠	٥	٠	٥	٠	٥	٠	٥
	٦	٠	٦	٢	٨	٤	٠	٦	٢	٨	٤
(c)*7 10 mod (النص العادي) ←	٧	٠	٧	٤	١	٨	٥	٢	٩	٦	٣
	٨	٠	٨	٦	٤	٢	٠	٨	٦	٤	٢
	٩	٠	٩	٨	٧	٦	٥	٤	٣	٢	١

ويوضح المثال في جدول (٧-٣) أهمية طول المفتاح في (التشفير بالمفتاح العام). فالمتسلل لن يستغرق وقتاً طويلاً في تخمين المفتاح الخاص (٧، ١٠) إذا كان على عِلم بالمفتاح العام (٣، ١٠). ومن ثم فإنه في الواقع العملي يتم استخدام أعداد كبيرة للغاية وذلك لمنع المتسللين من تخمين المفتاح الخاص في أي مدة زمنية معقولة.

خوارزمية (RSA):

يعتمد المثال في القسم السابق على نموذج مبسط لتوضيح الخصائص المميزة لـ (التشفير بالمفتاح العام). وتُعد خوارزمية (RSA) نوعاً من أنواع (التشفير بالمفتاح العام) المستخدم في الواقع العملي. وتعتمد خوارزمية (RSA) على الأُسس بدلاً من الضرب. وهذه الخوارزمية مشروحة باختصار في هذا المرجع[١٤].

(14) A method for obtaining digital signatures and public-key cryptosystems. Rivest, R.L., Shamir, A. and Adleman. L. Communications of the ACM, 1978,21(2): 120-126

١. ابدأ باثنين من الأعداد الأولية الكبيرة، ولنرمز لهم بـ (p) و(q). وتكون هذه الأرقام عادة أكبر من ٢٥٦ بت (bit) لكل منهما (أي أكثر من ٧٦ خانة عشرية لكل منهما).

٢. احسب (n = p*q)

٣. احسب (= (١-p) * (١-q) φ)

٤. اختر عدداً (e) يكون أولياً بالنســبة لـ (ϕ). مع ملاحظة أنه يجب ألا يوجد عوامل مشــتركة بين الرقمين باســتثناء العدد (١). (الحرف e يعني تشــفير-encryption- وهذا الرقم سيستخدم في التشفير).

٥. اخــتر عــدداً (d) يكون النظير الضربي لـ (e mod) بحيث أن أي رقم من هذا القبيل (d*e-1) يقبل القســمة على (ϕ).(الحرف d يعني فك التشفير-decryption-وهذا الرقم سيستخدم في فك التشفير).

٦. الزوج <e,n> يمثل المفتاح العام ويُستخدم في التشفير.

٧. الزوج <d,n> يمثل المفتاح الخاص ويُستخدم في فك التشفير.

٨. المفاتيح تستخدم كالتالي:

- لتشفير الرسالة (m)، احسب النص المشفر ($c = m^e \bmod n$).

- لفك شفرة النص المشفر (c)، احسب ($m = c^d \bmod n$).

ويمكن أن نطبق ذلك على مثال مبســط. لكن يجب أن يكون الشــخص فَطِناً في الأرقام التــي يختارها لأن الأســس ســتؤدي إلى أرقام ضخمة بسرعة كبيرة. ومــع ذلك فإن الأرقام التالية ستعمل بشكل جيد (p=3) (q=11)[١٥]. وباختيار هذه الأرقام سيكون لدينا:

1. (n = 3*11 = 33).

2. (φ) = 10*2 = (1-11) * (1-3) = 20).

---

(١٥) هذه الأرقام تم اختيارها في الكتاب التالي: Tannenbaum, A.S. and Steen, M.v. Distributed Systems: Principles and Paradigms. 2002. Upper Saddle River, NJ, Prentice-Hall, Inc

٣. لنفــرض أن (e) = ٣ لأنــه لا يوجــد عوامل مشــتركة بين العــدد (٣) والعدد (٢٠) باستثناء العدد (١).

٤. وبإمكاننا اختيار العدد (d) = ٧ لأن (3*7-1 = 20) والعدد ٢٠ يقسم (φ) = ٢٠.

٥. وبهذه الخيارات فإن:

- (c = m3 mod 33).

- (m = c7 mod 33).

الجدول (٧-٤): مثال على خوارزمية (RSA)

النص العادي			النص المشفر		النص العادي	
عملية المُرسِل				عملية المُستقبِل		
الرمز	التمثيل الرقمي (m)	m^3	m3 mod 33	c^7	c^7 mod 33	الرمز
H	8	512	17	410338673	8	H
E	5	125	26	8031810176	5	E
L	12	1728	12	35831808	12	L
O	14	2744	5	78125	14	O
I	9	729	3	2187	9	I
S	19	6859	28	13492928512	19	S
M	13	2197	19	893871739	13	M

ويوضح جدول (٧-٤) استخدام هذه الخيارات في مثال على خوارزمية (RSA). ويبدأ المثال بتحويل النص العادي إلى شــكل رقمي. وببساطة يستخدم المثال ترتيب الحروف الهجائية لتحديــد التمثيــل الرقمي، مثــلاً (a) = ١، (b) = ٢، وهكذا. ويمكــن التحقق من عمليات التشفير وفك التشفير من الجدول.

بمـا أن المفتاح العام يتضمن العدد (n) وهو حاصل ضرب العدد (p) والعدد (q) والتي تـم اختيارهما في البداية، فـإذا أمكن تحليل العدد (n) إلى عواملـه الأولية فإن خوارزمية (RSA) يمكن اختراقها. ولذلك فإن أمن خوارزمية (RSA) يعتمد بشكل حاسم على صعوبة تحليل الأعداد الكبيرة إلى عواملها الأولية.

أيضـاً تعتمد خوارزمية (RSA) بشـكل كبير على توفر أعداد كبـيرة من الأرقام الأولية الكبيرة. وإذا لم يكن كذلك، فإن المتسـلل يتمكن ببسـاطة من إنشاء جدول يتضمن جميع الأعداد الأوليـة المعروفة، ومن ثم محاولة تجريب حاصل ضرب هذه الأعداد حتى يتمكن من الحصول على العدد (n). لحسـن الحظ فإن الأعداد الأولية كثيرة، ولكن تخزين جميع الأعـداد الأولية المعروفة أمرٌ غير عملي. وبناءً على ذلك إذا تم اسـتخدام أرقام أولية كبيرة فإن خوارزمية (RSA) تكون آمنة على الأقل حتى الوقت الراهن.

نظرية العدد الأولي

احتمال أن العدد (n) يكون أولياً هو تقريباً $\frac{1}{\ln(n)}$ حيث تمثل (ln) اللوغاريتم الطبيـعي. وهذا أيضاً مساوٍ لـ $\frac{1}{2.3\log(n)}$ حيث تمثل (log) لوغاريتم الأساس ١٠. ولنفرض أن (n) عدد يتكون من ١٠ خانات. وبما أن ($\log(10^{10})=10$) فإن احتمال أن العدد يكون أولياً ($1/2.3 * 10 = 1/2.3$). وإذا كان العدد (n) يتكون من ١٠٠ خانة فإن احتمال أن العدد أولي يصبح ١ في ٢٣٠.

وبعبارة أخرى إذا قمنا باختيار ٢٣٠ عدد يتكون كل منهم من ١٠٠ خانة فمن المرجح جداً أن نعثر على عدد أولي. وبالتعاقب يوجد تقريباً $١٠^{٩٧}$ ($١٠^{١٠٠}/٢٣٠$) عدد أولي يتكون من ١٠٠ خانة. ويصل حجم تخزين الأجهزة الحاسوبية في العالم إلى قرابة $١٠^{٢٠}$ بايت، ولذلك فمن غير العملي تخزين جميع الأعداد الأولية لاختراق خوارزمية (RSA) باستخدام طريقة التخمين والاختبار.

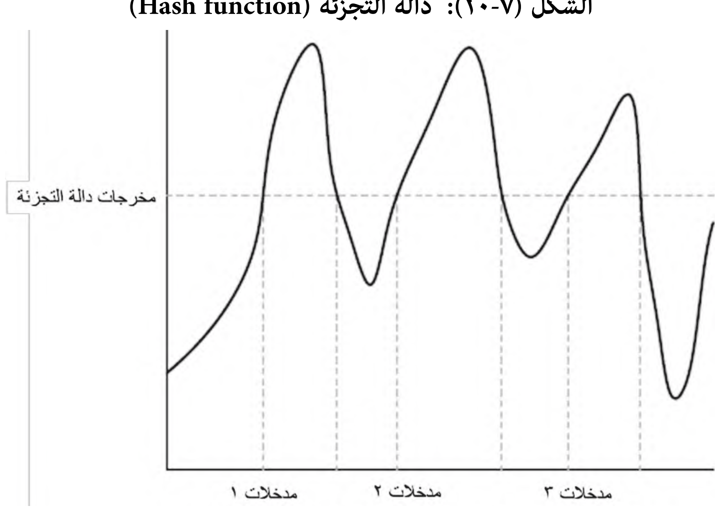
دوال التجزئة (Hash functions):

تُستخدم دوال التجزئة لتحويل المدخلات إلى مخرجات ذات طول ثابت. ولهذا التحويل خاصيتـان: (١) كل عنـصر مـن المدخلات يقابله عنـصر فريد من المخرجـات، (٢) ومن المسـتحيل تخمين أحد المدخلات بناءً على المخرجات المحددة. وهذا موضح في الشكل (٧-١٠). ويمكن ملاحظة أن جميع المدخلات لها مخرجات فريدة (وهذا هو سبب تسمية هذا التحـول بالدالة)[١٦]. لكن المدخلات من ١ إلى ٦ تـم تحويلها جميعاً إلى مخرجات التجزئة

(١٦) الدالة: قاعدة توافق بين مجموعتين بحيث يتم إسناد كل عنصر فريد من المجموعة الثانية إلى عنصر محدد في المجموعة الأولى (Houghton-Mifflin Harcourt eReference).

نفســها. ومن ثم عند تحديد مخرجات التجزئة فإنه من المســتحيل معرفة أن عنصراً معيناً من المدخلات قد أدى إلى المخرجات المحددة.

الشكل (٧-١٠): دالة التجزئة (Hash function)



وكما ناقشــنا ســابقاً فإن دالة التجزئة تُســتخدم أيضاً لحفظ كلمات المرور. فإذا كانت كلمة المرور محفوظة كنص واضح فإن سرقة البيانات تؤدي إلى الحصول على كلمات المرور. ومن ثم فإن حفظ كلمة المرور كدالة تجزئة يساعد على حمايتها من السرقة.

> بإمكانك أن تختبر هل يحفظ الموقع الإلكتروني كلمة المرور كنص واضح أو كدالة تجزئة من خلال طلب كلمة المرور. فإذا قام الموقع بإرسال كلمة المرور ستعرف حينها أن الموقع يحفظ كلمة المرور كنص واضح. أما إذا كان يحفظ كلمة المرور كدالة تجزئة فإنه لن يكون قادراً على إرسال كلمة المرور.

التشفير قيد الاستخدام:

التحدي المتبقي في اســتخدام التشــفير في الواقع العملي هو بناء الثقة في المفتاح العام المُرســل من قبل المستخدم. لقد رأينا أنه من الســهولة بمكان توليد المفتاح العام والمفتاح الخاص. لكن ما الذي ســيحدث إذا أرســل لك المُتسلل مفتاحاً عاماً وادعى أن ذلك المفتاح هو المفتاح العام للبنك الأمريكي (Bank of America). كيف ستكتشــف أن ذلك المفتاح ليــس تابعــاً لذلك البنــك؟ في الأجزاء المتبقية من هذا الفصل ســنناقش كيفية اســتخدام

(التشـفير بالمفتـاح العام) في التقنيات التجارية مثـل (SSL/TLS) و(VPNs). وبعد ذلك سنناقش الإجراءات المستخدمة لبناء الثقة في المفاتيح العامة.

تقنيات طبقة المنافذ الآمنة وبروتوكول أمن طبقة النقل (SSL/TLS) والشبكة الافتراضية الخاصة (VPNs):

التقنيات الأكثر شـيوعاً لتشفير المعلومات خلال النقل الشبكي هي تقنية «طبقة المنافذ الآمنـة وبروتوكـول أمـن طبقـة النقـل» (Security Sockets Layer and Transport Layer Security) (SSL/TLS) وتقنيـة «الشـبكة الافتراضية الخاصة» (Virtual Private Network) (VPN). في (SSL/TLS) يتم تشـفير معاملة معينة مع خادم شبكة معين، أما في (VPN) فيتم تشفير جميع الاتصالات من جهاز الحاسب الآلي.

والسـمة البارزة لجميع تقنيات التشفير المستخدمة عملياً هي الجمع بين أفضل ميزات (التشـفير بالمفتاح السري) و(التشـفير بالمفتاح العام) لضمان تجربة ممتعة للمسـتخدم. ويتطلب (التشـفير بالمفتاح السري) الحد الأدنى من القدرات الحاسـوبية، لكنه يحتاج إلى تبادل المفتاح المشـترك بشكل آمن قبل البدء بالتواصل السري. أما (التشفير بالمفتاح العام) فيسـتنزف المـوارد الحاسـوبية للأجهزة لذا فإنه ليس من المناسـب تشـفير المحادثة كلها باستخدام المفتاح العام خصوصاً في الأجهزة الصغيرة. ومع ذلك حتى أبسط الأجهزة يمكنها استخدام (التشفير بالمفتاح العام) لفترة وجيزة بهدف تبادل المفتاح السري.

لذلـك فإنه في الممارسـات التجارية يبدأ التواصل الآمن بالخادم الذي يزود المسـتخدم بالمفتاح العام. بعد ذلك يستحدث المستخدم مفتاحاً سرياً محلياً ويقوم بتشفيره باستخدام المفتاح العام للخادم. وهذا ينهي اسـتخدام (التشـفير بالمفتاح العام) لهذا التواصل. ويتم تشفير جميع التعاملات اللاحقة باستخدام المفتاح السري المشترك.

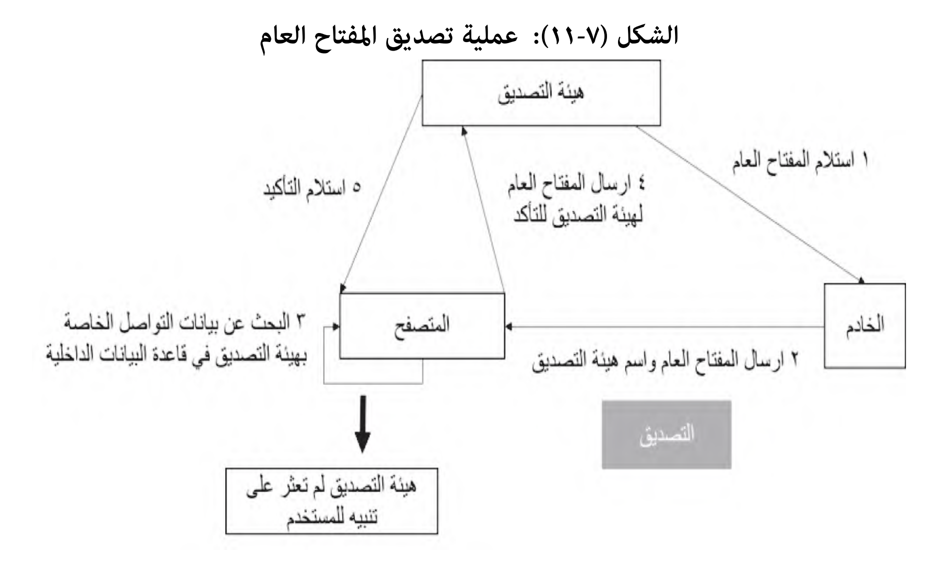
التصديق (Certificates):

عملياً التشـفير يعتمد بشـكل كبير على موثوقية المفتاح العام المُرسَل من قبل الخادم. وهـذا مماثل تمامـاً للحاجة لموثوقية رخصة القيادة كإثبات للهويـة في العالم المادي. ففي

العــالم المادي نتحقق من موثوقية رخصة القيادة من خــلال التأكد من أن الرخصة صادرة بالفعل من إدارة تســجيل المركبات في الولاية. أما في عالم الإنترنت فهناك شركات تُدعى بـ «هيئات التصديق» (certificate authorities) والتي تعمل بشــكل مشابه لإدارة تسجيل المركبــات حيث تصدر هيئة التصديق المفاتيح العامة للخــادم. وتتم عملية تبادل المفتاح العام كما هو موضح في الشكل (٧-١١).

وتحصــل الخوادم المهتمة بالمشــاركة في صفقات التجــارة الإلكترونية على المفتاح العام من أحــد مزودي المفاتيح العامة المعروفين بـ «هيئة التصديق» (certificate authority). وتقوم هيئة التصديق بتشفير المفتاح العام لخادم الشبكة وعنوان الـ (IP) وذلك باستخدام مفتاحها الخاص والذي يُستخدم كشهادة تصديق.

الشكل (٧-١١): عملية تصديق المفتاح العام



التوثيــق هــو مجموعة من المعلومــات تحتوي على المفتاح العام المشــفر للخادم، كما تحتوي على التعريف بمزود المفتاح. وتقوم الخوادم بإرســال التوثيق إلى العملاء للتعريف بأنفســهم قبــل البدء بالاتصال الآمن. ويــأتي العميل (أو المتصفح) مُحمّــلاً بمفاتيح عامة لجميع هيئات التصديق المعروفة. وإذا كانت هيئة التصديق معروفة فإنه يتم فك شــفرة التصديق باســتخدام المفتاح العــام المعروف والتابع لهيئة التصديــق. ويحتوي التصديق،

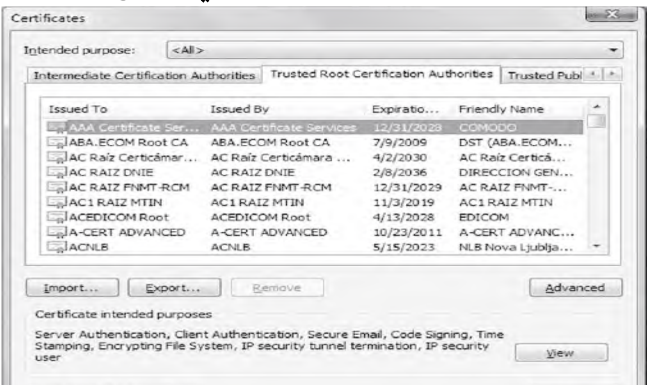
الذي تم فك شـــفرته، على المفتاح العام التابع لخادم الشبكة. وللتأكد من أن كل شيء على مـــا يرام، يقوم المتصفح أيضاً بمقارنة عنوان الـ (IP) التابع لخادم الشـــبكة بعنوان الـ (IP) التابع للخادم المتصل به المتصفح[١٧]، [١٨].

البنية التحتية للمفتاح العام (PKI):

الحلقة المفقودة الأخيرة في هذه العملية هي هيئات المصادقة. ما الذي يمنع المتســـلل من أن يتنكر في شكل هيئة مصادقة؟

طريقـــة تعاملنـــا مع هذا الموضوع هـــي أن المتصفحات تأتي بقائمة مـــن هيئات المصادقة التي تمت الموافقة عليها. والشـــكل (٧-١٢) يوضح مثالاً من متصفح كروم (Chrome). وإذا كان التوثيـــق الذي قدمه الخـــادم واحداً من تلك المذكورة في القائمة، فإن المتصفح يســـتخدم معلوماتـــه للتواصل مع هيئة التوثيق للتأكد مـــن صحة التوثيق. وإذا كان التوثيق صادراً من منظمة أخرى (على ســـبيل المثال، من الجامعة نفســـها)، يقوم المتصفح بتنبيه المستخدم حول هذه المسألة وذلك للسماح للمستخدم بالاعتماد على حكمه الشخصي في الثقة بهيئة التوثيق.

الشكل (٧-١٢): هيئات المصادقة في المتصفح



---

(١٧) ولتفاصيل أكثر، انظر الموقع التالي: http://www.moserware.com/2009/06/first-few-milliseconds-of-https.html، (accessed 2/2/13)

(١٨) ولتفاصيل مثيرة للاهتمام حول عملية تشفير التوثيق على أساس الميثولوجيا الهندوسية، انظر المقال التالي: «Alice and Bob can go on a holiday,» by S. Parthasarthy. http://profpartha.webs.com/publicationslalicebob.pdf (accessed 07/18/2013). وقد يكون هناك أمثلة أخرى توضيحية وذات علاقة بثقافة محددة ومشابهة لما سبق. نرغب في معرفة تلك الأمثلة لإدراجها في الطبعات القادمة من هذا الكتاب (مع الإسناد طبعاً).

ويوضح الشـكل (٧-١٣) مثالاً عـلى أحد تلك التنبيهات. وتم إصـدار التوثيق في هذه الحالة على خادم ويب محلي بواسطة هيئة مصادقة تُدعى (Nessus). ولأن خادم الشبكة هذا ليس من ضمن هيئات المصادقة المعروفة، فإن المسار الحكيم للمتصفح هو أن يطلب من المستخدم المشورة بخصوص كيفية التعامل مع هذه الحالة.

ويُطلق على الإطار الذي أُنشئ لإصدار توثيقات المفاتيح العامة والحفاظ عليها وإلغائها «البنية التحتية للمفتاح العام» (public-key infrastructure).

نموذج حالة - شركة (Nation Technologies):

لقد رأينا في هذا الفصل أن الطريقة الأساسـية التي نسـتخدمها للتشفير هي تأمين قناة الاتصال. وتسـمح لنا التقنيات مثـل «طبقة المنافذ الآمنة وبروتوكـول أمن طبقة النقل» (SSL/TLS) وتقنية «الشـبكة الافتراضية الخاصة» (VPN) بإنشاء اتصال مشفر بين أجهزة الحاسـب الآلي، لكن المحتوى نفسـه يظل دون تشفير. أما التقنيات الأخرى المستخدمة في التشفير فتقوم بتشفير القرص الصلب بالكامل.

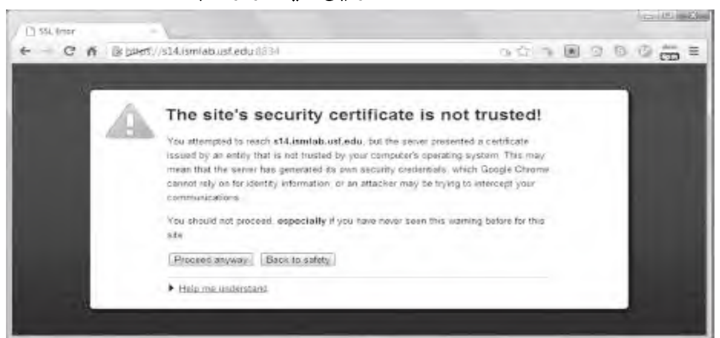
والمشـكلة المشتركة في جميع طرق التشـفير هذه هو أنه على الرغم من محاولة تشفير المعلومات المحفوظة في الملفات، فإن هذه الطرق تقوم بتشـفير كل شيء باسـتثناء الملفات نفسها. وبمجرد أن يقوم المستخدم بتسجيل الدخول على حسابه فإن جميع الملفات تكون مرئيـة. فيمكن لهجوم انتحالي (phishing attack)، الذي يسـتهدف المسـتخدم الموجود حالياً على النظام، أن يحصل وبنجاح على جميع الملفات التي يسـتطيع المستخدم الوصول إليها. فبمجرد أن يتم إرسـال الملف عبر البريد الإلكتروني فإن المُرسل لا يتمكن من التحكم في كيفية قيام المُستقبل بحماية المحتويات المعلوماتية في الملف.

هل سـيكون من الأسـهل الاكتفاء بتشـفير الملفات التي تحتاج إلى تشـفير؟ وهل من الأفضل جعل الملفات مشفرة طوال الوقت، وتركها دون تشفير خلال فترة القراءة والتحرير وذلك لمستخدمين محددين؟

هـذه التقنيـة ممكنـة وقد تـم تطويرهـا من قبـل شركة تُدعـى شركـة (Nation Technologies)، والتي أسسها ستيفن نيشن (Stephen Nation)، وهو ضابط استخبارات

ســابق في إدارة شرطة مدينة نيويورك (NYPD). وتسمح منتجات وخدمات هذه الشركة للعملاء بتشــفير الملفات منفردة بعضها عن بعض. ويمكن تبادل الملفات المشــفرة مع أي عدد من المستخدمين. ويستطيع الشخص الذي يشفر الملف أن يحدد أذونات الوصول إلى الملفات وذلك لمســتخدمين محددين، بحيث يكون كل مســتخدم مُحدداً من خلال عنوان بريده الإلكتروني أو أي مُعرِّف آخر. ويمكن لمُســتقبلي الملفات حفظ الملف وفتحه للقراءة، وعندما يتم إغلاق الملف فإنه يعود إلى حالته المشفرة. والميزة المُحتملة لهذه الطريقة هي أنه لا يكون لدى المنظمات ما يدعو للقلق بشأن سرقة أسرارها لأن المعلومات تكون مشفرة حتى وهي محفوظة.

الشكل (٧-١٣): توثيق غير موثوق به



الملخص:

في هذا الفصل ناقشــنا موضوع التشــفير على المســتويات العليا من حيث التطبيقات والخوارزميات والبنية التحتية القائمة لتمكين التشــفير السَلِس. وقد ناقشنا ثلاثة أنواع من التشــفير: دوال التجزئة، والتشفير بالفتاح السري، والتشفير بالمفتاح العام. وتختلف أنواع التشفير من حيث عدد المفاتيح المستخدمة في التشفير.

وعملياً تجمع التقنيات المســتخدمة مثل (VPN) و(SSL) بين التشــفير بالمفتاح السري والتشــفير بالمفتاح العام. ويُســتخدَم التشــفير بالمفتاح العام مبدئياً لتبادل المفتاح وذلك لتجنب استنزاف الموارد الحاســوبية التي تحدث إذا استُخدم التشفير بالمفتاح العام لكامل المعاملة.

وحتـى تتم عملية التبادل بسلاسـة، أنشـئت صناعـة تقنية المعلومـات مجموعة من الإجـراءات للتحقق من المفتـاح. وهذه الإجراءات تُعرف مُجتمعة باسـم «البنية التحتية للمفتـاح العام». ويمكـن أن يُقاس نجاح هذه الإجراءات بالجهل النسـبي لمُعظم العملاء بالأنشطة التي تجري في الخلفية لضمان أمان معاملات التجارة الإلكترونية.

توصية:

لنقاش جذاب ومرح وشامل حول التعامل مع التشفير ننصح بشدة بقراءة كتاب كوفمان وبيرلمان وسبيسـينر[١٩]، إذ إن جميع تفاصيل التشـفير التي لم نتحدث عنها في هذا الفصل يمكن استكمالها بالرجوع إلى هذا الكتاب. وبالإضافة إلى كون المؤلفين من أكثر الناس دراية عـن هذا الموضوع، فإنهم خبراء وكُتاب موهوبون قد بذلوا جهداً كبيراً لجعل هذا الموضوع التقني موضوعاً شـخصياً وسـهل التناول. وقد تعلمنا، نحن مؤلفي كتاب (أمن المعلومات وإدارة مخاطر تقنية المعلومات)، كثيراً من هذا المرجع.

أسئلة مراجعة للفصل:

١. ما التشفير؟
٢. ما استخدامات التشفير؟
٣. باختصار اشرح شفرة قيصر.
٤. ما متطلبات خوارزمية التشفير الجيدة؟
٥. لماذا تُستخدم المفاتيح في خوارزميات التشفير الحديثة؟
٦. ما التشفير بالمفتاح السري؟
٧. قـدّم لمحـة عامة عن المعيـار الحالي لـ (التشـفير بالمفتاح السـري). ما هي بعض تطبيقات هذا المعيار؟

---

(19)Kaufman, c., Perlman, R. and Speciner, M., 2002. Network Security: Private Communication in a Public World, Prentice-Hall

٨. ما التشفير بالمفتاح العام؟

٩. ما هي بعض تطبيقات التشفير بالمفتاح العام؟

١٠.ما التوقيعات الرقمية؟

١١.كيف يُستخدم (التشفير بالمفتاح العام) لتجهيز التوقيعات الرقيمة؟

١٢.ما دوال التجزئة؟ قدّم لمحة عامة عن دوال التجزئة المشهورة.

١٣.ما استخدامات دوال التجزئة؟

١٤.ما تشـفير المجموعة؟ ولماذا يتم تجزئة البيانات إلى مجموعات للقيام بـ (التشـفير بالمفتاح السري)؟

١٥.ما الاستبدال في سياق التشفير؟

١٦.ما الإحلال في سياق التشفير؟ ولماذا نحتاج إليه؟

١٧.ما نموذج الخلط والنشر في التشفير؟

١٨.ما تسلسل تشفير المجموعات؟ وما أهميته؟

١٩.قدّم لمحة عامة عن خوارزمية (RSA).

٢٠.ما تقنية «طبقـة المنافذ الآمنة وبروتوكول أمن طبقـة النقل» (SSL/TLS) وتقنية «الشبكة الافتراضية الخاصة» (VPNs)؟ وما استخداماتها؟

٢١.ما هي بعض الاختلافات بين (SSL) و (VPNs)؟

٢٢.ما التوثيق؟

٢٣.ما هيئات التوثيق؟ وما الخدمات التي تقدمها؟

٢٤.ما البنية التحتية للمفاتح العام (PKI)؟

٢٥.لماذا نحتاج البنية التحتية للمفتاح العام (PKI)؟

أسئلة على نموذج الحالة:

١. قــم بزيارة الموقع الإلكــتروني لشركــة (Nation Technology) (www.nationtech nologies.com). ما هي بعض ميزات منتجات الشركة؟

٢. اعتماداً عــلى رأيك، صِف إحدى الطرق المفيدة لاســتخدام التقنية التي توفرها شركة (Nation Technology).

٣. اعتماداً على رأيك، ما الشركات وما الصناعة التي تنتمي إليها يمكن أن تستفيد أكثر من غيرها من التقنية التي توفرها شركة (Nation Technology)؟ ولماذا؟

٤. في اعتقادك ما أهم مخاطر الأعمال التي تواجهها شركة (Nation Technology)؟

نشاط التدريب العملي - التشفير:

هذا النشــاط العملي يوضح استخدام التشفير اعتماداً على آلة لينكس الافتراضية والتي تم إعدادها في الفصل الثاني. وســوف تقوم بتنفيذ التشــفير باســتخدام دوال التجزئة (٠ مفتــاح)، والمفتــاح الــسري (١ مفتاح)، والمفتاح العــام (٢ مفتاح). تأكــد أن لديك اتصالاً بالإنترنت، وافتح نافذة طرفية لإكمال هذه الأنشطة.

كلمات مرور دوال التجزئة:

كــما ذكر خــلال هذا الفصل أن أنظمة التشــغيل تحفظ نتائــج دوال التجزئة بدلاً من حفــظ القيمــة الحقيقية لكلمة المــرور. وفي نظام (CentOS Linux) فــإن دالة التجزئة الافتراضيــة لكلــمات المرور هــي (SHA-512) (وفي الماضي كانــت (DES) و(MD5) هي الدوال الافتراضية).

- قم بتسجيل الدخول باستخدام حساب (alice) (كلمة المرور: aisforapple) وافتح نافذة طرفية.
- يحتوي نظام (CentOS) على برنامج (grub_crypt) والذي يسمح لنا برؤية نتائج دوال التجزئة المختلفة دون تغيير كلمة مرور المستخدم.

```
[alice@sunshine  Desktop]$   grub-crypt
--sha-512
Password:  aisforapple
Retype password:  aisforapple
$6$DqW2UfDcPZjKyQyc$fwQqIAxfEgEuy6
KFAKxEdKP1cWuy0d5vemqNRV2uNAPf1VNaX
hpmZYOIZuW8iitC82MhQMaR2h8EY0DgQb5Z/1
[alice@sunshine   Desktop]$   grub-crypt
--sha-256
Password:  aisforapple
Retype password:  aisforapple
$5$omu31sk0zLzOVug12$sbFJlcupATlu6Kw2iTf
qXMMbbgYanXoNtEDjgVH876
[alice@sunshine Desktop]$ grub-crypt --md5
Password:  aisforapple
Retype password:  aisforapple
$1$S213Gc1H$sTKjWuHbrSrquDLzy4XT8/
```

وتحتوي النتائج على ثلاث قيم مفصولة بعلامة الدولار. ويمكن تفسير هذه النتائج كما يلي (idsalt$hash):

القيمــة الأولى (Id) - وهــي مُعرّف رقمي يحــدد خوارزمية دالة التجزئة المســتخدمة (MD5, SHA-256, SHA-512)[٢٠].

- القيمــة الثانية (Salt) - سلســلة من الأحرف العشــوائية المُســتخدمة لزيادة طول مدخلات الدالة.
- القيمــة الثالثة (Hash) - نتيجة خوارزمية دالــة التجزئة على كل من: كلمة المرور الخاصة بالمستخدم والقيمة الثانية (salt).

---

(٢٠) لقائمة كاملة من الخوارزميات المعتمدة راجع صفحة (pam_unix man) على الرابط، /http://linux.die.net pam_unix/٨/man

وكــما ترى فإن الخوارزميــات المختلفة تؤدي إلى نتائج مختلفة بشــكل كبير حتى عند استخدام كلمة المرور نفسها كمدخلات.

اخــتر كلمة مــرور قوية بناءً على القواعــد المذكورة في الفصل الثامن، ثُم قم بتشــغيل برنامج (grub-crypt) مع دوال التجزئة (MDS)، و(SHA-256)، و(SHA-512).

قم بتشغيل الأمر (grub-crypt) عدة مرات مع استخدام كلمة المرور نفسها وخوارزمية التشفير.

أسئلة:

١. هل يؤدي تشغيل الأمر عدة مرات إلى النتائج نفسها في كل مرة؟ علل إجابتك.

٢. احفظ نتائج الأمر السابق في ملف نصي بالامتداد التالي:

/opt/book/encryption/results/ex١.txt

النتائج المطلوب تسليمها: قم بتسليم محتويات الملف (ex1.txt) إلى أستاذ المادة.

ملف دالة التجزئة «المجموع الاختياري» (checksum):

وبالإضافــة إلى كلمات المرور فإن الاســتخدام الرئيسي لخوارزميــة دالة التجزئة في نظام لينكــس هو التحقق من تكامل ملفات الأنظمة. ويعد الأمر (md5sum) وســيلة ســهلة لتوليــد «المجموع الاختيــاري»[٢١] لملف معتمداً على خوارزميــة (MD5)، أو لمقارنة ملف بمجمــوع اختياري معروف مســبقاً. وإذا كان «المجموع الاختيــاري» للملف يختلف عن كل القيــم الجيدة والمعروفة، فإن الملف قد تم تعديله مما يعني أن النظام قد تم اختراقه. وبالإمكان توليد «مجموع اختياري» لملف كما يلي:

```
[alice@sunshine ~]$ md5sum hello.txt
8ddd8be4b179a529afa5f2ffae4b9858 hello.txt
```

«المجموع الاختياري» المُعتمِد على خوارزمية (MD5) يســتند كذلك إلى محتويات الملف، ومن ثم يمكن نســخ الملف أو إِعادة تسميته دون التأثير في قيمة المجموع الاختياري، لكن إذا تم تعديل المحتويات بأي شكل من الأشكال فإن الأمر (md5sum) سيُعطي قيمة مختلفة.

(٢١) يوجد أوامر لتوليد «المجموع الاختياري» اعتماداً على خوارزمية (SHA) لكن خوارزمية (MD٥) هي الأكثر استخداماً في الواقع العملي.

```
[alice@sunshine ~]$ cp hello.txt world.txt
[alice@sunshine ~]$ md5sum world.txt
8ddd8be4b179a529afa5f2ffae4b9858   world.
txt
[alice@sunshine ~]$ echo '!' >> world.txt
[alice@sunshine ~]$ md5sum hello.txt world
txt.
8ddd8be4b179a529afa5f2ffae4b9858 hello.txt
c231742ea29c9e53d4956d8fa4dd6d96 world.txt
```

كما يمكن حفظ مخرجات الأمر (md5sum) على شكل ملف نصي، وهذا سيكون مفيداً في حال توليد «المجموع الاختياري» لعدد كبير من الملفات حيث يمكن بعد ذلك اســتخدام الملــف النصي كمدخــلات لمفتاح (c) في الأمــر (md5sum)، والذي يقــارن بين «المجموع الاختياري» لجميع ملفات وتقارير النتائج المذكورة.

```
[alice@sunshine ~]$ md5sum *.txt > check-
sums.txt
[alice@sunshine ~]$ cat checksums.txt
8ddd8be4b179a529afa5f2ffae4b9858 hello.txt
c231742ea29c9e53d4956d8fa4dd6d96 world.txt
[alice@sunshine ~]$ echo 'This has been
modified' > hello.txt
[alice@sunshine ~]$ md5sum -c checksums.
txt
hello.txt:  FAILED
world.txt:  OK
md5sum:  WARNING:  1 of 2 computed check-
sums did NOT match
```

أسئلة:

الملـــف التـــالي (/opt/book/encryption/checksum/checksums.txt) يحتوي على قائمـــة من «المجمـــوع الاختياري» المُعتمِد على خوارزميـــة (MD5) لجميع الملفات في هذا الدليل. تحقق من تكامل الملفات.

١. سَـجّل جميع الملفات التي تفشـــل في اختبار التحقق من تكامـــل الملفات في الملف التالي (/opt/book/encryption/results/failed.txt).

٢. أنشئ ملفاً نصياً يحتوي على جميع قيم «المجموع الاختياري» للملفات ذات الامتداد (.png) في هذا الدليل وقم بحفظه كما يـــلي (/opt/book/encryption/results/checksum.txt).

النتائج المطلوب تسليمها: قم بتسليم محتويات الملف (failed.txt) وملف (checksum.txt) إلى أستاذ المادة.

التشفير بالمفتاح السري:

يُســـتخدم التشـــفير بالمفتاح السري على نطاق واســـع في نظام لينكس لتشفير الملفات. وتشـــمل معظم توزيعات لينكس الحديثة دعماً لواحد أو أكثر من نُظم الملفات المشـــفرة، والتي تقوم بتشـــفير جميع الملفات كما هي مكتوبة في القرص. ويعد موضوع تهيئة نظام الملفات المشـــفرة خارج نطاق هذا الفصل، لكن الأمر (aescrypt)[٢٢] يوفر وســـيلة لحماية الملفات الفردية بنفس طريقة التشـــفير بالمفتاح السري. وقائمة مُعامِلات الأوامر سهلة جداً كما هو موضح في الجدول (٧-٥).

وبالإمكان استخدام هذه الأوامر لتشفير وفك تشفير ملف (hello. txt) كما يلي:

```
[alice@sunshine ~]$ cat hello.txt
Hello World!
[alice@sunshine ~]$ aescrypt -e hello.txt
p 1234qwer -o hello.txt.aes-
```

(٢٢) ليس مدرجاً في التثبيت الموحد لنظام (CentOS) لكنه متاح في الموقع التالي: http://www.aescrypt.com

الجدول (٧-٥): خيارات الأمر (aescrypt)

مُعامِلات الأوامر	الوظائف
-e	تشفير الملف
-d	فك تشفير الملف
-p <password>	كلمة المرور المستخدمة. وإذا كان هذا الخيار محذوفاً، فإن هذا الأمر يقوم بتسجيل دخول المستخدم بشكل فوري.
-o <filename>	ملف المُخرجات

```
[alice@sunshine ~]$ head -1 hello.txt.aes
AES^B^@^@^XCREATED BY^@AESCRYPT
3.05^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^@^
@^@^@@^@
[alice@sunshine  ~]$ aescrypt -d hello.
txt.aes -p 1234qwer -o
hello.decrypt.txt
[alice@sunshine ~]$ cat hello.decrypt.txt
Hello World!
```

أسئلة:

في هذا التمرين قم بتغيير الأدلة إلى (/opt/book/ encryption/secret-key).

١. قم بتشفير الملف (plans. txt) باستخدام كلمة المرور (pinky) واحفظ المخرجات في الملف (/opt/book/encryption/results/plans.aes).

٢. قم بفك تشــفير الملف (encrypted. aes) باستخدام كلمة المرور (brain) واحفظ المخرجات في الملف (/opt/book/encryption/results/plaintext.txt).

النتائج المطلوب تسليمها: قم بتسليم محتويات الملف (plans.aes) وملف (plaintext. txt) إلى أستاذ المادة.

التشفير بالمفتاح العام باستخدام (GPG)[٢٣]:

(GPG) هـــي اختصار لـــ (GNU Privacy Guard)، وهو برنامج مجاني بديل لبرنامج Pretty Good Privacy (PGP) والذي يستند إلى معيار (OpenPGP). لكن هذا يقودنا إلى السؤال التالي: ما هو برنامج (PGP)؟

تــم تطوير برنامج (PGP) من قبل فيليب زيمرمــان (Phillip Zimmerman) في عام ١٩٩١. وكان (PGP) أول برنامج تشفير تم بناؤه على خوارزمية التشفير بالمفتاح العام، بما في ذلك خوارزمية (RSA) والتي ناقشــناها في هذا الفصل. وبسبب قضايا براءات الاختراع تم إنشاء معيار (OpenPGP) وذلك لتحديد صيغ البيانات القياسية للتشغيل المتبادل بين برمجيات التشفير. ويُعد (GPG) واحداً من أكثر البرمجيات شيوعاً والتي تم تطويرها بناءً على هذا المعيار. ويســمح لك برنامج (GPG) بتشــفير البيانات، والتوقيع عليها، وإرسالها إلى الآخرين بحيث يســتخدم هؤلاء الأشــخاص المفتاح العام الذي توفره لهم لفك تشــفير البيانات.

ولاســتخدام التشفير بالمفتاح العام قمنا باســتحداث زوج من المفاتيح. ويتوجب عليك مشاركة المفتاح العام، كما يتوجب عليك استخدام زوج المفاتيح للتشفير وفك التشفير.

استحداث المفاتيح:

الخطوة الأولى في نظام التشــفير بالمفتاح العام هي توليد زوج المفاتيح (العام/الخاص). ويوفر برنامج (GPG) مفتاح (genkey) والذي سيقوم بهذه العملية.

```
[alice@sunshine ~]$ gpg --gen-key
gpg (GnuPG) 2.0.14; Copyright (C) 2009
Free Software Foundation, Inc.
This is free software: you are free to
change and redistribute it.
There is NO WARRANTY, to the extent per-
mitted by law.
```

(٢٣) نتقدم بالشكر لـ «كلايتون ايتلو» (Clayton Whitelaw)، وهو طالب في كلية علوم الحاسب الآلي وعضو في نادي طلاب (Whitehatters) في جامعة جنوب فلوريدا، على تأليفه للنسخة الأولية من هذا القسم.

وســوف يُطلب منك أن تختــار أي نوع من المفتــاح الذي تريــده للتوقيعات الرقمية والتشــفير. اخــتر الخيار الافــتراضي (RSA and RSA). وبعد ذلك ســيُطلب منك اختيار حجم المفتاح. والحجم الافتراضي هو ٢٠٤٨ بت. وبإمكانك بأمان اختيار هذا الخيار. بعد ذلك ســتختار طول صلاحية المفتاح. وفي حالات الواقع العملي هذه القيمة تكون بين سنة وخمس سنوات، لكن لهذا التمرين لا حاجة لتحديد مدة زمنية لصلاحية المفاتيح.

```
Please select what kind of key you want:
   (1) RSA and RSA (default)
   (2) DSA and Elgamal
   (3) DSA (sign only)
   (4) RSA (sign only)
Your selection? 1
RSA keys may be between 1024 and 4096 bits
long.
What keysize do you want? (2048) 2048
Requested keysize is 2048 bits
Please specify how long the key should be
valid.
        0 = key does not expire
      <n> = key expires in n days
      <n>w = key expires in n weeks
      <n>m = key expires in n months
      <n>y = key expires in n years
Key is valid for? (0) 0
Key does not expire at all
Is this correct? (y/N) y
```

بعد ذلك ســيُطلب منك اختيار اســم للمفتاح، وعنوان البريــد الإلكتروني، والملاحظات. وبإمكانك اســتخدام اسمك الحقيقي وعنوان بريدك الإلكتروني الفعلي في هذا التمرين. أما

بالنســبة للملاحظات فبإمكانك كتابة اسم المنظمة-مثلاً (Sunshine State University). وسيقوم برنامج (GPG) باستخدام الملاحظات لإنشاء زوج المفاتيح.

```
GnuPG needs to construct a user ID to
identify your key.
Real name:  Alice Adams
Email address:  alice@sunshine.edu
Comment:  Sunshine State University
You selected this USER-ID:
        «Alice Adams (Sunshine State»
University) <alice@sunshine.edu>»
Change (N)ame, (C)omment, (E)mail or (O)
kay/(Q)uit? O
```

ســتحتاج إلى إدخال كلمة مرور. كما ســيظهر لك مربع حوار مشابه لما في الشكل (٧-١٤). أدخــل كلمة مــرور تتميز بأنها آمنة ويمكنك تذكرها. وأخيراً ســيبدأ البرنامج باســتحداث المفاتيح الخاصة بك. ولزياد فاعلية المفتاح، من الجيد أن تقوم بتحريك الفأرة في اتجاهات عشــوائية، أو أن تقوم بتنفيذ بعض المهام على جهاز الحاســب الآلي في حين يقوم البرنامج باســتحداث المفاتيح. وقد يســتغرق اســتحداث المفاتيح ثواني أو دقائق لأن ذلك يختلف اختلافاً كبيراً تبعاً لعدة عوامل.

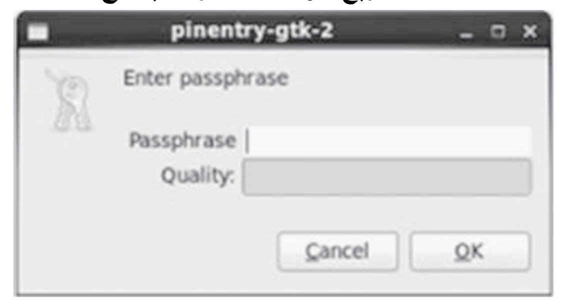
وبمجرد اكتمال هذه العملية، فإنك تكون استحدثت أول زوج مفاتيح خاص بك.

> نحتاج إلى توليد الكثير من وحدات البايت العشوائية. ومن ثم فمن الجيد أن تقوم بتنفيذ بعض الإجراءات الأخرى (كالطباعة على لوحة المفاتيح، وتحريك الفأرة، واستخدام الأقراص) خلال الاستحداث الأولي للمفاتيح. وهذا يعطي مولد الأرقام العشوائي فرصة أفضل للحصول على ما يكفي من العشوائية.

```
gpg: key 9ED0CE35 marked as ultimately
trusted
public and secret key created and signed.
gpg: checking the trustdb
gpg: 3 marginal(s) needed, 1 complete(s)
needed, PGP trust model
gpg: depth: 0 valid: 1 signed: 0 trust:
0-, 0q, 0n, 0m, 0f, 1u
pub   2048R/14382D17 201201-12-
      Key fingerprint = B317 3F83 705B
889D B414 7DF0 A3C1 B094 7E5B 6F3F
uid          Alice Adams (Sunshine State
University) <alice@sunshine.edu>
sub 2048R/C8761AAB 201201-12-
```

ما قمنا به في الأقسام السابقة هو إنشاء زوج مفاتيح، ومكان هذا الزوج في مجلد مخفي يدعــى (gnupg.) في الدليــل الرئيسي. وهذا المجلد مع بعــض المحتويات الأخرى بما في ذلك (pubring. gpg) و(secring. gpg) تحتوي على المفتاح العام والمفتاح الخاص على التوالي. وكلا الملفــين محفوظ في صيغة ثنائيــة (binary format) ومن ثم لا يمكنك قراءة محتوياتها لكن برنامج (GPG) يستطيع تفسير هذا الملف وعرض المعلومات التي تحتاج إليها.

الشكل (٧-١٤): مربع حوار كلمة المرور لبرنامج (GPG)



مشاركة المفاتيح:

لعرض المفاتيح العامة المحفوظة في حافظة المفاتيح التابعة لبرنامج (GPG)، اكتب الأمر التالي:

```
[alice@sunshine ~]$ gpg --list-keys
/home/alice/.gnupg/pubring.gpg
------------------------------
pub   2048R/14382D17 201201-12-
uid                 Alice Adams (Sunshine
State University) <alice@sunshine.edu>
sub 2048R/C8761AAB 201201-12-
```

ولعرض المفاتيح الخاصة، اكتب الأمر التالي:

```
[alice@sunshine ~]$ gpg --list-secret-keys
/home/alice/.gnupg/secring.gpg
------------------------------
sec   2048R/14382D17 201201-12-
uid              Alice Adams (Sunshine
State University) <alice@sunshine.edu>
ssb   2048R/C8761AAB 201201-12-
```

وقبل أن تتمكن من تبادل البيانات المشـــفرة مع الآخرين، عليك أن تفعل شيئين: أعط الآخرين نسخة من المفتاح العام التابع لك، وقم باستيراد نسخة من المفتاح العام التابع لهم في برنامج (GPG). ولتصدير المفتاح العام التابع لك كملف نصي قُم بما يلي:

```
[alice@sunshine ~]$ gpg -a -o /tmp/alice_
adams.pub --export
[alice@sunshine ~]$ head /tmp/alice_
adams.pub
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version:  GnuPG v2.0.14 (GNU/Linux)
```

mQENBFC6Q/MBCACjZH9O43XeK8TfDXVW084xmr2
lgiLsv7drbT9poQiuHmHrnbAm
I/dm+nTIQn4qI8d+qTn0oWUsa9HD+N5sAsAHkYl5
kkmWgg/rtP8NtaH84/qqKSQN
ktmd/zxfyNgJ4fTHhfqJA6RuHoKuFla+MMqKzR4u
+ZSjxgmHl4tbSBph2+YgmMp8
fqLH18i4fSEoG5jZ6VciPw8KAyZvVIsC5TyOfX-
W67UU8QJ7bEZaejxMtrhecF4F/

الآن إذا تــم تصدير المفتاح العــام التابع لك، يتوجب عليك أن تُعطيه للشــخص الذي ســتتبادل المعلومات معه. وعملياً ســيتم إرســال المفتاح عبر البريد الإلكتروني إلى الطرف الآخر، أو يتم مناولة المفتاح يداً بيد إلى المستلم في الحالات الأمنية المشددة للغاية.

ملاحظة:
إذا كان لديك مفاتيح متعددة، مثلاً مفتاح للاستخدام الشخصي وآخر لاستخدام العمل، يمكنك تحديد أي مفتاح تريد أن تُدرِج باستخدام الرمز (u-) <user> حيث <user> هو عنوان البريد الإلكتروني للمفتاح الذي تريد استخدامه.

في حالتنا هذه قد تم بالفعل نقل المفتاح إلى مســتخدم آخر في جامعة ولاية الشــمس المشرقة وهو (bob@sunshine.edu)، كما قام هذا المســتخدم باستيراد المفتاح وحفظه في حافظة المفاتيح التابعة لبرنامج (GPG). وقام بوب (Bob) أيضاً باســتحداث زوج المفاتيح وأخبرنا بأنه يمكننا الحصول عليها في (/home/bob/public_html/bob_brown.pub) أو (http://www.sunshine.edu/-bob/bob_brown.pub). لذلك لدينا خيارين لاســتيراد المفتاح العام التابع لبوب: استيراد ملف من نظام الملفات المحلي كما يلي:

```
[alice@sunshine ~]$ gpg --import /home/
bob/public_html/bob_brown.pub
gpg:  key 310C3E16:  public key «Bob Brown
(Sunshine State University)
<bob@sunshine.edu>» imported
gpg:  Total number processed:  1
gpg:       imported:  1 (RSA:  1)
```

أو استيراد الملف من خادم الشبكة البعيد كالتالي:

```
[alice@sunshine ~]$ gpg --fetch-keys
http://www.sunshine.edu/~bob/bob_brown.
pub
gpg:  key 310C3E16:  public key «Bob Brown
(Sunshine State University)
<bob@sunshine.edu>» imported
gpg:  Total number processed:  1
gpg:            imported:  1 (RSA:  1)
```

وفي كلتا الحالتين سيكون لديك المفتاح العام لاستخدامه.

كن حذراً عند استيراد المفاتيح العامة من مضيف بعيد، والتي تتم عن طريق شبكة الإنترنت أو البريد الإلكتروني. يجب أن تتأكد من حصولك على المفتاح العام الصحيح، وأنه لم يتم العبث به أو تعديله، قبل استخدامك إياه في أي اتصال آمن.

وإذا قمت بتشغيل الأمر (gpg - - list-keys) مرة أخرى، فسوف تجد المفتاح العام التابع لـ (Bob Brown) في قائمة المفاتيح المتاحة:

```
[alice@sunshine ~]$ gpg --list-keys
/home/alice/.gnupg/pubring.gpg
------------------------------
pub 2048R/14382D17 01-12-2012
uid            Alice Adams (Sunshine
State University)
<alice@sunshine.edu>
sub   2048R/C8761AAB  01-12-2012

pub   2048R/310C3E16  01-12-2012
uid           Bob Brown (Sunshine State
University)
<bob@sunshine.edu>
sub   2048R/1EA93238   01-12-2012
```

التشفير وفك التشفير:

وبما أنك الآن تملك المفتاح العام، ســتكون قادراً على تشــفير الرسالة بالطريقة التي تم تصميمها لمستلم معين. وللتوقيع على ملف وتشفيره، عليك أولاً حفظه في هيئة ملف نصي (لأن الصيغــة الافتراضية هي الصيغة الثنائية). ثم اســتخدم المفتاح (a) والمفتاح (e) وقم بتحديد الشخص الذي سيستخدم (المفتاح العام) وذلك عن طريق المفتاح (r) كما يلي:

```
[alice@sunshine ~]$ gpg -s -a -r bob@sun-
shine.edu -e hello.txt
you need a passphrase to unlock the secret
key for
user:   «Alice   Adams   (Sunshine   State
University) <alice@sunshine.edu>»
2048-bit RSA key, ID 14382D17, created
  01-12-2012
```

بعــد ذلك يقوم برنامج (GPG) بعرض مربع حــوار لإدخال كلمة مرور أليس (Alice) التابعــة للمفتاح الخاص. وبمجرد إدخال كلمة المرور يقوم برنامج (GPG) بفحص حافظة المفاتيح بحثاً عن المفتاح العام التابع لـ (bob@sunshine.edu):

```
gpg:  1EA93238:  There is no assurance this
key belongs to the named user
```

```
pub 2048R/1EA93238  01-12-2012 Bob Brown
(Sunshine State University) <bob@sun-
shine.edu>
Primary key fingerprint:  599F 4790 E781
ADBF 1850 F120 2B51 B871 310C 3E16
Subkey fingerprint:  26BF DCFC 0A62 7224
9D20 5DE5 9734 A6C4 1EA9 3238
```

```
It is NOT certain that the key belongs to
the person named in the user ID.  If you
*really* know what you are doing, you may
answer the next question with yes.
```

```
Use this key anyway? (y/N) y
```

ويقوم برنامج (GPG) بإصدار تحذير بأن مفتاح بوب (Bob) قد لا يكون جديراً بالثقة لأنــه تم اســتيراده حديثاً، وفي الوقت ذاتــه لا يوجد معلومات في حافظــة المفاتيح التابعة لبرنامج (GPG) يُمكن استخدامها للتحقق من صحة المفتاح. يمكنك بأمان أن تتجاهل هذه الرســالة، لكن إذا كنت تُخطط لاســتخدام برنامج (GPG) في عملك، فعليك بمراجعة دليل الخصوصية التابع لـ (GNU)[٢٤] وذلك للحصول على مزيد من المعلومات حول بناء «شبكة من الثقة» (Web of Trust) في إدارة المفاتيح.

```
[alice@sunshine ~]$ cat hello.txt.asc
-----BEGIN PGP MESSAGE-----
Version:  GnuPG v2.0.14 (GNU/Linux)
```

(24) https://www.gnupg.org/gph/en/manual.html

hQEMA5c0psQeqTI4AQgAgpJ4Z4hiN93q+DdZ2ETg
nm1ib+ciekRGmNtI4C5KMzPm
b C W u s 0 c q m t L W E L 6 D j 4 o M 9 0 H B G 9 D i -
iNKxrxKdjAneh9i/AYVf3/UleyW0Zb2dL/
dC
v e C x l k N a G L C t K j V 0 9 6 7 e w /
J s H B Q b V 1 2 j X R n q N 6 1 r m p /
edFIQZ1tbXymXlcnfg3vm
a R K n K S s X V a 0 q O H x P P n 0 +s k P 6 t F b M T /
q / 5 F 1 D f p I f 9 N Y 1 m V L J D i M N Q G p y y 2 /
ZZyKk
90PWxBsQC90CcWTfJqwjC1wPd4Ck2YOr+q6u36YR
hz8cLwoM9I3MR2xVbtdElTGy
Zd2ogWZImTRBxhKWYV7uVDre095Y4FNIzbzADZ1
KaNLAwgGGslcOrrCI4gpSkGIb
DbvhuIr1r2rKeBRxR3dbQ+xb6Wm9S8v8440VSLDD
D4f3TZFc6+/qUlAW7fU9Xu/1
4nqN4nu9NCQLgWmZyLtJr8RIry0tVxHQwhOQl-
2w6t34b0IZJvjLGzkmM589fwWNo
ggE3krRiBvAE17z101Ncqn/zu5bfc6BUD2Okc-
36Qg56NUzvydGM3xgK2FRwgQfhr
7 T r s J p / 9 R +w X V 6 E G f T u o T o A /
p1WY5311952l2Wrd7e2nwm6umeaKxgzgO4hrC9zS
k576lCUi0cPyhwWBHQdK8UtssmBH1+tt2hEa6H+b
Tf1OIOZptMU64NCG3rWgrI17
N W n t q 9 w w W Q T 5 a g q C a l t h L F M 4 7 n i /
m K e 5 1 K a y 9 L c k N U m m
5PC8yA4oti5jnpIaW4Jw
xRFvTSoRXH5ARlPc1INoNi+51X+jd8y9AB2096s2
x+BQFuCmG25K/z7E2BoJjsVV
zf/qg6yQTbgPmvG83Jyvev71ykXd7TfKZGs4UlKq
K+grJda8
=BxNI
-----END PGP MESSAGE-----

والآن بعد أن قمت بتشفير رسالة إلى بوب (Bob) وقمت بالتوقيع عليها بالمفتاح الخاص، حان الوقت بالنسبة لبوب (Bob) لفك تشفير الرسالة. وبالإمكان تبديل المستخدمين إلى حساب بوب (Bob) ومن ثم فك تشفير الملف لاختبار هذه العملية.

```
[alice@sunshine ~]$ su - bob
Password:
[bob@sunshine ~]$ gpg -o hello.txt
--decrypt ~alice/hello.txt.asc
You need a passphrase to unlock the secret
key for
user:  «Bob Brown (Sunshine State
University) <bob@sunshine.edu>»
2048-bit RSA key, ID 1EA93238, created
201201-12- (main key ID 310C3E16)
```

ويجب أن تشاهد الآن مربع حوار إدخال كلمة المرور. وعند إدخال كلمة مرور بوب (Bob) التابعة للمفتاح الخاص (bisforbanana)، سيتم فك تشفير الملف لكن ستتلقى رسالة تفيد بوجود خطأ عند التحقق من التوقيع:

```
gpg:  encrypted with 2048-bit RSA key, ID
1EA93238, created 201201-12-
«Bob Brown (Sunshine State University)
<bob@sunshine.edu>»
gpg:  Signature made Sun 02 Dec 2012
10:37:18 AM EST using RSA key ID 14382D17
gpg:  Can't check signature:  No public key
```

ويجب أن يقوم بوب (Bob) باستيراد المفتاح العام التابع لأليس (Alice) قبل التحقق من التوقيع الموجود على الملف:

```
[alice@sunshine ~]$ gpg --import /tmp/
alice_adams.pub
gpg: key 14382D17: public key «Alice
Adams (Sunshine State University) <alice@
sunshine.edu>» imported
gpg: Total number processed: 1
gpg: imported: 1 (RSA: 1)
```

قم بتجريب أمر فك التشــفير مرة أخرى وفي هذه المرة سيتم فك التشفير وسيتم حفظ المحتويات في ملف (hello. txt). بعد ذلك سيقوم برنامج (GPG) بالتحقق من التوقيع:

```
gpg: Signature made Sun 02 Dec 2012
10:37:18 AM EST using RSA key ID 14382D17
gpg: Good signature from «Alice Adams
(Sunshine State University) <alice@sun-
shine.edu>»
gpg: WARNING: This key is not certified
with a trusted signature!
gpg:         There is no indication that
the signature belongs to the owner.
Primary key fingerprint: C42E 0E23 08A1
8116 019A AAB3 2D73 7113 1438 2D17
```

ومرة أخرى يقوم برنامج (GPG) بإصدار إنذار لأن حافظة المفاتيح التابعة لبرنامج (GPG) ليــس لديها معلومات كافيــة للتحقق من المفتاح العــام التابع لــ (alice@sunshine.edu). وبمجرد الانتهاء مــن التحقق من التوقيع، بإمكانك التأكد من أن محتويات الملف الذي تم فك شفرتها صحيحة.

```
[ bob@sunshine ~]$ cat hello.txt
Hello World!
```

أسئلة:

١. قم باستحداث زوج من المفاتيح العامة والخاصة باستخدام اسمك وعنوان بريدك الإلكتروني، وفي حقل الملاحظات استخدم اسم جامعتك.

٢. قم بتصدير المفتاح العام وحفظه كما يلي: (/opt/book/encryption/results/key.pub).

٣. قم باستيراد المفتاح العام المحفوظ في ملف (/opt/book/encryption/public-key/eric_pierce.pub).

٤. اذكر المفاتيح العامة والخاصة المخزنة في حافظة المفاتيح التابعة لبرنامج (GPG) واحفظ المخرجات كما يلي على التوالي: (opt/book/encryption/results/public-keyring.txt) و(opt/book/encryption/results/private-keyring. txt).

٥. قم بتشفير الملف التالي والتوقيع عليه (/home/alice/hello. txt) باستخدام المفتاح العام الذي قمت باستيراده في الخطوات السابقة واحفظ المخرجات كما يلي (/opt/book/ encryption/results/ encrypted.asc)

النتائج المطلوب تسليمها: قم بتسليم محتويات الملفات التالية إلى أستاذ المادة:

(key.pub)،و(public-keyring.txt)، و(private-keyring.txt.)،و(encrypted.asc).

تمرين التفكير النقدي - مفاتيح التشفير المتضمنة لنماذج العمل:

في هذا الكتاب لم نقض الكثير من الوقت في نقاش الحوسبة السحابية وبالتحديد المخاطر المنبثقة من وضع الكثير من البيانات في السحابة. هل تعلم أين تكون بيانات بريدك الإلكتروني التابع لـ (Gmail)؟ أو هل تعلم أين تحفظ شركة مايكروسوفت الملفات التي تقوم أنت بتخزينها في خدمة (Sky Drive)؟

ربما أنك لا تهتم كثيراً بذلك، وهذا هو الشيء المعقول الذي يقوم به كثير من الناس. إن الشركات ستخسر الكثير في حال فقدها لثقة الجمهور. لذا فإن نموذج العمل الحالي

قائم أساســاً على أن المستخدمين يثقون في مقدمي الخدمات السحابية المجانية مع إيمانهم بــأن مزودي الخدمات الســحابية قد يلقون نظرة خاطفة عــلى محتويات الملفات لأغراض محدودة. ويبدو أن تخصيص الإعلانات عبر الإنترنت أحد هذه الأغراض المعقولة. ومن ثم تتم مقايضة خدمة التخزين السحابية المجانية في مقابل الإعلانات عبر الإنترنت.

لكن ومنذ الكشف عن التعاون بين مزودي خدمات الحوسبة السحابية وبين وكالة الأمن القومي (NSA)، بدأ بعض المســتخدمين بالشــعور بالقلــق إزاء خصوصية معلوماتهم. ما الذي يستطيع المستخدمون فعله إذا ما زالوا يرغبون في الاستفادة من الخدمات السحابية؟

مما قرأناه في هذا الفصل يبدو أن الحل سهل. حالياً يتكفل مقدمو الخدمات السحابية بالتشــفير. أي أن من يملك مفاتيح تشــفير البيانات هم مقدمو الخدمات السحابية وليس أصحاب البيانات. وهذا يسمح لمقدمي الخدمات السحابية برؤية بياناتك بناءً على طلبهم. ومن ثم فإن ملكية مفاتيح التشــفير من قِبــل مزودي الخدمة تتضمن نموذج العمل التالي: (الإعلان في مقابل التخزين).

وإذا أردت منــع ذلك بإمكانك تشــفير بياناتك قبل رفعها إلى مزود الخدمة الســحابية. وبعد ذلك ستكون أنت المسؤول عن إدارة المفاتيح لأنك إذا فقدت مفاتيح فك التشفير فلن تكون قادراً على قراءة بياناتك.

المراجع:

Falkenrath, R. «Op-ed: encryption, not restriction, is the key to safe cloud computing,» http://www.nextgov.com!cloud-computing12012/1O/op-ed-encryption-not-restriction-key-safe-cloud-computing/586081 (accessed 0711812013

Amazon Web Services, «Using client-side encryption,» http://docs.aws.amazon.com!AmazonS3/1atestldevlUsingClientSideEncryption.html (accessed 07118/2013)

Schneier, B. Cryptogram, November 15,2012

أسئلة على تمرين التفكير النقدي:

١. تُقدَّم العديد من خدمات الحوسبة السحابية المشهورة مثل الجيميل (Gmail) مجاناً لأن المستخدمين يسمحون بالإعلانات التجارية في مقابل الخدمات المجانية. في اعتقادك كيف سيكون تطور سوق الخدمات السحابية إذا تم تشفير الكثير من البيانات بحيث لا يتمكن مزودو الخدمات السحابية من الاستفادة المالية من بياناتك عن طريق الإعلانات التجارية؟

٢. ما هي بعض الاهتمامات الخاصة للجهات المُنظِمة مثل الوكالات الحكومية عندما يتعلق الأمر بالحوسبة السحابية؟ (الموقع الإلكتروني لـ (Nextgov op-ed) يوضح بعض الأمثلة على ذلك).

تصميم حالة:

يُعد قسم القبول في جامعة ولاية الشمس المشرقة نشط للغاية في مجال استقطاب الطلاب. ويقوم القسم بصورة دورية بزيارات للمدارس الثانوية المحلية بهدف الترويج لبرامج الجامعة. كما يقوم القسم في كثير من الأحيان بجمع معلومات الطلاب الشخصية بهدف مساعدتهم في التقديم على المنح الدراسية، والمساعدات المالية، والفرص الأخرى.

ومن أجل تسجيل كل هذه المعلومات، يقوم الموظفون أثناء زيارتهم بحمل أجهزة الحاسب الآلي المحمولة التابعة للجامعة. ومؤخراً تعرضت إحدى سيارات هؤلاء الموظفين للسطو والسرقة. ولحسن الحظ فإن الجاني لم يسرق جهاز الحاسب الآلي المحمول الذي كان في صندوق السيارة (والذي يحتوي على ٥٠٠ رقم من أرقام الضمان الاجتماعي للطلاب).

ولأنك خبير في أمن المعلومات، تواصل معك رئيس الجامعة ليسألك عن رأيك فيما يمكن عمله لجعل أجهزة الحاسب الآلي المحمولة أكثر أمناً. وأثناء قراءتك لقوانين الولاية أدركت أنه في حال تشفير كامل القرص في أجهزة الحاسب الآلي المحمولة فإن سرية المعلومات الواردة في الأجهزة ستكون محمية ومن ثم لا حاجة للإبلاغ عن الحادثة.

اكتب توصياتــك لرئيس الجامعة في صفحة واحدة بحث تغطــي المعلومات الواردة في الفقرة الســابقة، وتناقش موضوع شراء الجامعة لحلول تســاعد على تشــفير كامل القرص. ويجب أن يشمل تقريرك معلومات حول ما يلي:

١. تقرير عن المتطلبات القانونية لمثل هذا التشفير في الجامعات الحكومية في ولايتك.

٢. الخطوط العريضة حول متطلباتك لهذا المُنتج.

٣. القيام ببعض البحث على الإنترنت حول العروض المشهورة لهذا المُنتج بحيث يتضمن ما لا يقل عن ثلاثة من الموردين.

٤. اشرح الفرق بين تشفير الملفات وتشفير كامل القرص.

٥. متى يجب أن يُستخدم تشفير الملفات، ومتى يجب أن يستخدم تشفير كامل القرص؟ (مع الأخذ بعين الاعتبار الأمور التي يســتطيع كل من تشــفير الملفات وتشفير كامل القرص حمايتها).

٦. ما أنظمة التشغيل التي ستركز عليها في نقاشك؟

٧. كيف سيتم استرداد مفتاح فك التشفير في حال ضياعه؟

الفصل الثامن

إدارة الهوية والوصول

نظرة عامة:

في هذا الفصل سـنُلقي نظرة على أكثر الآليات شـيوعاً في تحديد المسـتخدمين وإدارة امتيازاتهم في الأنظمة المؤسساتية. وتتسم الأنظمة التي سوف نناقشها بالعديد من الميزات المشتركة، لكن تم تطوير كل نظام منها للاستجابة لاحتياجات محددة وظروف معينة. وفي نهاية هذا الفصل يجب أن تعرف:

- الفرق بين إدارة الهوية وإدارة الوصول.
- مراحل نماذج إدارة الهوية وإدارة الوصول.
- الفئات الثلاث لبيانات اعتماد المستخدم.
- نقاط القوة ونقاط الضعف النسبية للتقنيات الرئيسية للمصادقة.

إدارة الهوية:

إدارة الهوية هي عمليات تحديد هوية الأفراد وجمع كل البيانات اللازمة لمنح أو إلغاء امتيازات مستخدمي الموارد الحاسوبية. ويُعد نظام (اسم المستخدم) و(كلمة المرور) الذي تسـتخدمه على جهاز الحاسـب الآلي المحمـول الخاص بك مثالاً لنظـام إدارة الهوية. وفي المنظـمات الكبيرة أصبحت العمليات الرسـمية ضرورية لإدارة أعمال المسـتخدمين الكثيرة باسـتخدام الأنظمة الحاسـوبية. وبالاعتماد على مثال من جامعة حكومية نموذجية، ففي كل يوم هناك المئات من الأنشـطة، مثل انضمام الطلاب للجامعة، وترك الطلاب للجامعة، والحصول على عمل في الحرم الجامعي، وتغيير في وظائف الموظفين في الحرم الجامعي، فكل هذه الأحداث تؤثر في المعلومات التي يجب أن يُسـمح لهؤلاء المستخدمين بالوصول إليها. فالعمليات البسـيطة المُتبعة مع جهاز الحاسـب الآلي المنزلي يجـب أن يحل محلها أنظمة

رســمية للتأكد أن كل شخص لديه معلومات حديثة في هذه البيئة الديناميكية وذلك دون المســاس بالمعلومــات التي لا ينبغي لهــم الوصول لها. وتقوم أنظمــة إدارة الهوية بالمهام اللازمة لتحقيق هذه الأهداف.

ويتم تخزين معلومات المســتخدمين في نظام الســجلات (system of record). وبناء عــلى قانون الخصوصيــة لعــام ١٩٧٤[1] (US Privacy Act) يُعرف نظام الســجلات بأنه الســجلات التي يمكن من خلالها اســترداد المعلومات بالاســم، أو رقم الهوية، أو الرمز، أو أي مُعــرِّف مُحدد عــلى وجه الخصوص للفرد. ولا يجب أن يكون نظام الســجلات مفصلاً جداً. وتُعد لوحة المســتخدم في جهاز الحاســب الآلي المعتمد على نظام ويندوز أحد أمثلة نظام الســجلات. كما يمكن اعتبار قواعد بيانات الموارد البشرية والرواتب أحد أمثلة نظام الســجلات. ففــي المنظمات الكبيرة قد تكون قواعد البيانــات تلك جزءاً من نظام تخطيط موارد المؤسســة (ERP system)، لكن في المنظمات الصغيرة قد تكون قواعد البيانات تلك على شكل جداول بيانات إكسل (Excel spreadsheet).

وبالمثــل فإن نظــام معلومات الطالب الجامعي هو مثال على نظام الســجلات لبيانات الطلاب. وكقاعدة عامة يتم إنشاء نظام السجلات لحفظ البيانات لغرض محدد أو لمجموعة محددة من الأشخاص. على سبيل المثال يتم العثور على معلومات حول الطالبة التي تعمل في الجامعة في نظام سجلات الطلاب ونظام سجلات الموظفين. ومن ثم فإنه من الشائع أن يكون لشخص منفرد عدة هويات في أنظمة سجلات متعددة في الوقت ذاته.

وفي نظام الســجلات، الهوية هي ســجل محدد محفوظ في نظام السجلات. إذاً فإن ما نُســميه عادة «مستخدم جهاز الحاسب الآلي» يُطلق عليه «هوية» في عالم أمن المعلومات. أمــا المُعرِّف فهو عبارة عن سلســلة من الأرقام التي تُعرِّف بشــكل فريــد الهوية في نظام السجلات.

وتتعامــل أنظمــة إدارة الهوية مــع التعقيــدات المتعلقة بمزامنة الهويــات مع أنظمة السجلات. وتعمل هذه الأنظمة في مراحل ثلاث (الشكل ٨-١) لجمع كل المعلومات اللازمة لإدارة الهويات - اكتشــاف الهوية، ملاءمة الهوية، وإثــراء الهوية. وفي نهاية هذه العملية

(1) http://www.justice.gov/opcl/privstat.htm

نحصل على سجل الشخص (Person Registry) مع معلومات عملية حول المستخدمين في المنظمة.

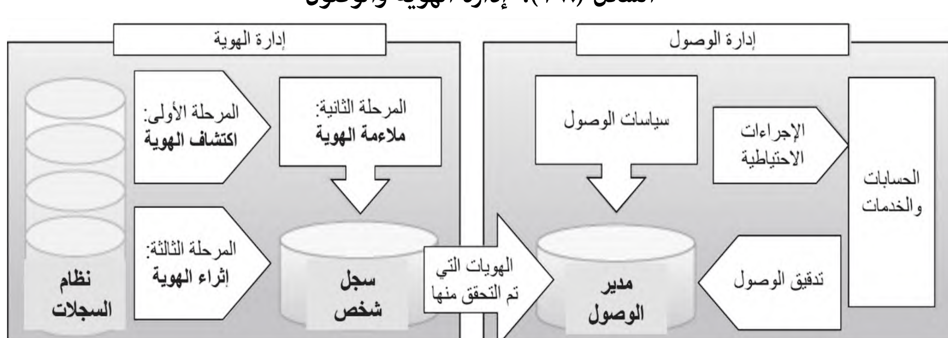
المرحلة الأولى: اكتشاف الهوية:

تبدأ إدارة الهوية بمرحلة الاكتشاف، حيث يتم إيجاد جميع الهويات الجديدة والمُحدثة في جميع أنحاء المنظمة. وفي هذه المرحلة يقوم نظام إدارة الهوية بجمع كل المُعرفات الجديدة والمُحدثة في جميع أنظمة السجلات. فتغييرات الأسماء، وتحديثات الأدوار، وتصحيحات تواريخ الميلاد أو المعرفات كلها أمور شائعة الحدوث ويجب أن يتم اكتشافها. وتختلف تعقيدات هذه المرحلة إلى حد كبير على حجم المنظمة. ففي المنظمات الصغيرة ذات التسرب الوظيفي المنخفض، يمكن أن تكون هذه العملية يدوية بالكامل عندما يتم التعاقد مع الموظف أو إنهاء عقده، يتم تحديث بيانات الموظف في قاعدة بيانات الموارد البشرية وإدخالها يدوياً في نظام إدارة الهوية. لكن في المنظمات الضخمة قد تتضمن هذه العملية نُظماً آلية متعددة تقوم بجمع آلاف الوحدات من البيانات من عشرات من الأنظمة أو أكثر، ويتم ذلك عدة مرات في يوم واحد. وبغض النظر عن الطريقة، ففي نهاية مرحلة اكتشاف الهوية نحصل على قائمة مُعرِّفات جديدة أو مُحدَثة من جميع نظم السجلات في المنظمة. وتُمثل هذه القائمة مدخلات المرحلة القادمة من عملية إدارة الهوية - ملاءمة الهوية.

المرحلة الثانية: ملاءمة الهوية:

بمجرد أن يتم تجميع قائمة المُعرِفات الجديدة والمُحدثة، يمكننا القيام بملاءمة الهوية. وملاءمة الهوية هي عملية مقارنة كل هوية مُكتشفة مع سجل رئيسي وذلك لجميع الأشخاص في المنظمة.

الشكل (٨-١): إدارة الهوية والوصول



ولإيضاح أهمية ملاءمة الهوية، افترض قيام جامعة ولاية الشمس المشرقة بالتعاقد مع عضو هيئة تدريس جديد. يتم إدخال البيانات التالية في قاعدة بيانات الموارد البشرية في الجامعة:

القسم	تاريخ الميلاد	اسم العائلة	الاسم الأول	الرقم التعريفي
علم الآثار	٠٣/١٣/٢٠	جونز	هنري	١٣٥٧٩

وبعد بضع سنوات قرر الدكتور جونز (Dr. Jones) أن يَدرس في وقت فراغه وقرر أن يُسجل مادة من قسم الأحياء. وبناء على ذلك يتم إدخال البيانات التالية في نظام معلومات الطالب:

الصف	تاريخ الميلاد	اسم العائلة	الاسم الأول	الرقم التعريفي
أحياء ١٠١	٠٣/١٣/٢٠	جونز	هنري	٢٤٦٨٠

فبدون القيام بعملية ملاءمة الهوية فإنه ليس من الواضح إذا كان هناك شخصان يحملان اسم هنري جونز (Henry Jones) أحدهما عضو هيئة تدريس والآخر طالب، أو أن هناك شخصاً واحداً لكن بأدوار متعددة وذلك عندما يتم جمع المُعرفات من أنظمة السجلات المُتعددة في مكان واحد.

الدور	اسم العائلة	الاسم الأول	الرقم التعريفي
عضو هيئة تدريس	جونز	هنري	١٣٥٧٩
طالب	جونز	هنري	٢٤٦٨٠

ومن خلال القيام بعملية ملاءمة الهوية نستطيع معرفة أن كلا السجلين يعود للشخص نفسه المدعو هنري جونز (Henry Jones)، على النحو التالي:

تاريخ الميلاد	رقم الموظف	رقم الطالب	اسم العائلة	الاسم الأول	الرقم التعريفي
٠٣/١٣/٢٠	١٣٥٧٩	٢٤٦٨٠	جونز	هنري	١٣٥٧٩

سجل الشخص (Person Registry):

كما ترى في المثال السابق فقد صدر لهنري جونز (Henry Jones) مُعرِّف جديد بالإضافة إلى مُعــرِف الموظف ومُعــرِّف الطالب التي صدرت من نظام الســجلات التابعة لها. وهذا المُعــرِّف الثالث يتبــع لنظام إدارة الهوية حيث يوجد في قلب معظــم أنظمة إدارة الهوية قاعدة بيانات تُدعى بـ سجل الشخص (Person Registry). و «سجل الشخص» هو المحور المركزي الذي يربط المُعِرفات من جميع نظم السجلات في هوية رئيسية واحدة، ويجعل من ارتباط وانتقال بيانات الهوية (مثل الرقم الجامعي والرقم الوظيفي) أمراً ممكناً.

مم يتكون سجل الشخص؟ السجل في حد ذاته هو مجرد قاعدة بيانات بسيطة. وتقوم قاعــدة البيانات تلك بإصدار مُعرِّف فريد لكل شــخص يتم اســتحداثه في قاعدة البيانات. لاحظ أن هذه المُعرِّفات تصدر «لكل شــخص» وليس «لكل هوية» كما في نظام الســجلات. وكما رأينا في المثال أعلاه أنه يمكن أن يكون لكل شخص هويات متعددة في نظام السجلات، لكن الهدف من ســجل الشــخص هو إصدار مُعرِّف واحد لكل شــخص. ويحفظ ســجل الشــخص جميع المعرفات من أنظمة الســجلات المُختلفة، كما يحفــظ البيانات التعريفية الأخرى (كالاسم، وتاريخ الميلاد، وغيرها) وذلك لكل فرد في المنظمة.

وظائف ملاءمة الهوية:

تتميز عملية ملاءمة الهوية بثلاث وظائف رئيسـية: إنشـاء الهويـة، ومطابقة الهوية، ودمـج الهويـة. وفي الواقع فإنه يُشـار أحيانـاً إلى ملاءمة الهوية في الصناعـة بأنها عملية «المطابقـة والدمـج». مطابقة الهوية هي عملية البحث في السـجل الحالي للشـخص عن السـجلات التي تتطابق مع مجموعة معينة من بيانات الهوية. وبمجرد العثور على سـجل شـخص مُطابق فإن وظيفة «دمج الهوية» تدمج السـجل الجديد أو المُحدث مع البيانات المرتبطة بالسجل الحالي للشخص. وإذا لم يتم العثور على تطابق مناسب في سجل الشخص فإنه يُفترض أن البيانات المُقدمة تُمثل شـخصاً جديداً. وفي هذه الحالة يتم استدعاء وظيفة «إنشاء الهوية» والتي تقوم بإنشاء سجل جديد ومُعرِف جديد تابع له ويكون ذلك في سجل الشـخص. ويحدث تعارض إذا كانت بيانات الهوية المعينـة تتطابق مع هويات متعددة. ولحل مشكلة تعارض الهوية يجب على المسؤول تقييم بيانات الهوية المُقدمة من قبل نظام السجلات، ومن ثم يُقرر ما إذا كانت الهوية جديدة، أو يقوم المسؤول بمطابقة الهوية يدوياً مع هوية أخرى من الهويات الموجودة في النظام. ويوضح الشـكل (٨-٢) مخططاً انسيابياً لعملية المطابقة والدمج.

ومـرة أخرى فـإن تعقيد مرحلة ملاءمة الهوية يختلف اختلافـاً كبيراً وذلك عتماداً على حجم المنظمة وعلى عدد نظم السـجلات. وفي أبسـط الحالات، وهي المنظمة التي تحتوي على نظام واحد للسجلات، فإن عملية ملاءمة الهوية وسجل الشخص لا حاجة لهما. وعلى كل حـال فإنـه بعد الانتهاء من ملاءمة الهويات، يتم الانتقـال إلى المرحلة التالية في عملية إدارة الهوية وهي إثراء الهوية.

لماذا لا يتم استخدام أرقام الضمان الاجتماعي (social security numbers) كمُعرِفات في كل الأنظمة؟

السؤال الطبيعي في هذه المرحلة: لماذا لا نستخدم أرقام الضمان الاجتماعي في كل الأنظمة؟ فأرقام الضمان الاجتماعي تصدر بالنتيجة لكل فرد وليس لكل هوية. وهذا من شأنه القضاء إلى حد كبير على الحاجة لملاءمة الهوية.

أحد الأسباب المهمة لعدم استخدام أرقام الضمان الاجتماعي على نطاق واسع هو أن استخدام هذه الأرقام على هذا النحو سيخلق عبئاً إضافياً على المنظمة للحفاظ على أمن هذه الأرقام.

المرحلة الثالثة: إثراء الهوية:

حتــى هذه النقطة في عمليــة إدارة الهوية فإن البيانات الوحيــدة التي تم جمعها من نظام الســجلات ترتبط بفرد محدد، وذلك لتمييز تلك البيانات عن بقية الأفراد الآخرين في المنظمــة. وتقــوم مرحلة إثراء الهوية بجمع بيانات عن علاقة كل فرد بالمنظمة. وفي مثالنا الســابق من جامعة ولاية الشــمس المشرقة، فإنه في مرحلة اكتشــاف الهوية قد تم جمع مُعرِفات هــنري جونز (Henry Jones) من قاعدة بيانات الطــلاب وقاعدة بيانات الموارد البشرية، لكن لم يتم جمع أي معلومات عن علاقة هذا الشخص بالجامعة. وفي أثناء مرحلة إثراء الهوية ســنقوم بتســجيل أن هنري جونز (Henry Jones) هو عضو هيئة تدريس في قســم علم الآثار كما أنه يدرس مادة في قســم الأحياء. وبعد مرحلة إثراء الهوية فإن سجل الشخص الخاص بهنري جونز سيكون كما يلي:

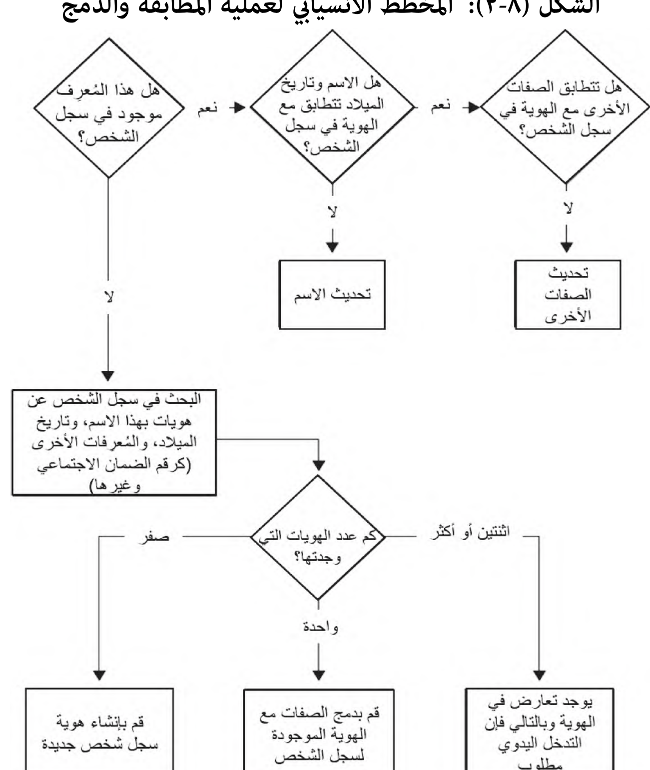
Identifier	First Name	Last Name	Student ID	Employee ID	Birth Date	Roles
987654	Henry	Jones	24680	13579	03/13/20	Faculty: Archaeolo(Student: Biology

ويُشار إلى علاقة الفرد بالمنظمة بدور الفرد وانتمائه للمنظمة. ويمكن أن يكون للأفراد أدوار متعددة في المنظمة، كما يمكن أن يكون لهم عدة أدوار في منظمات متعددة في وقت واحد. على ســبيل المثال، مدير التســويق في شركة ما يحمل دور المدير من حيث التسويق في المنظمة، كما يحمل دور الموظف من حيث الشركة بأكملها. ولهذا الســبب فإن معظم المنظــمات ترى من الضروري تحديد الدور الرئيسي لكل فــرد. ويتم إنجاز ذلك من خلال تطبيــق قيمة الأولوية لكل دور كجزء من عملية إثراء الهوية. وبمجرد تجميع قائمة الأدوار لكل شخص يمكن ترتيب القائمة بناءً على قيمة الأولوية والدور الرئيسي المُحدد. ففي المثال الســابق دور المدير ســيحصل على قيمة أولوية أعلى من دور الموظف، ولذلك فإنه الدور الرئيسي الذي سيتم تسجيله للمُستخدم سيكون «مدير». وبالمثل فإن الدور الرئيسي لهنري جونز (Henry Jones) سيكون «عضو هيئة تدريس».

وعنــد الانتهاء من مرحلة إثراء الهوية فإن عملية إدارة الهوية تكون قد اكتملت. ومن ثــم يكون نظام إدارة الهوية قد جمع ما يكفي من المعلومات في ســجل الشــخص ليكون

متأكداً بما فيه الكفاية من أنه تم تعريف كل فرد في المنظمة بشكل فريد، كما تم استرجاع الكثير مـن المعلومات لاتخاذ قرارات ذكية حول الوصول وحـول الامتيازات التي يجب أن يحصل عليها هذا الفرد. الآن الهوية جاهزة للاستخدام من قِبل نظام إدارة الوصول والذي يتعامل مع قرارات الوصول والأنشطة الناتجة عن ذلك.

الشكل (٨-٢): المخطط الانسيابي لعملية المطابقة والدمج



إدارة الوصول:

تُؤسـس عملية إدارة الهوية لمعرفة الأفراد في المنظمة. أما الآن فنحن بحاجة لمعرفة ما يُسـمح لكل من هؤلاء الأفراد بالقيام به. ويشـمل نظام إدارة الوصول جميع السياسـات، والإجراءات والتطبيقات التي تأخذ البيانات من سـجل الشـخص ونظام السـجلات بهدف اتخاذ قرار بشأن منح صلاحيات الوصول للموارد.

التحكم في الوصول المُعتمِد على الدور:

قبـل منـح صلاحيات الوصـول لأي من موارد المنظمـة يتوجب على مسـؤول الأمن وعلى قيادة المنظمة تطوير سياسـات لتنظيمٍ كيفية منح الوصول. وفي معظم المنظمات الكبيرة، تلك السياسات تستخدم نهج التحكم في الوصول المُعتمِد على الدور (role-based access control). وفي نظام التحكم في الوصول المعتمد على الدور، فإن الأذونات اللازمة لتنفيذ مجموعة من العمليـات المرتبطة ببعضها يتم اعتبارها دوراً من أدوار النظام. كما يتم ربط أدوار النظام تلـك بمهام وظيفة أو وظائف محـددة في المنظمة. ونظام التحكم في الوصول المُعتمِد على الدور يمنح الأفراد ذوي الأدوار المحددة امتيازات وصول تتناسـب مع أدوار النظام المناظرة لها. على سـبيل المثال، قد يُسـمح للشـخص الذي يعمل وكيل مشتريات بإدخال أمر شراء جديد، لكن لا يُسـمح له بالموافقة على الدفع بحيث تُمنح القدرة على الموافقة على الدفع لدور مرتبط بشـخص في وظيفة مختلفة مثل المحاسبة. وتعرف الحالة التي يقوم فيها أكثر من شـخص بإتمام مهمة كاملة بحالة فصل المهام. وتُعد حالة فصل المهام سـمة مشتركة في أنظمة الأعمال وخاصة عندما يتعلق الأمر بالمعاملات النقدية.

ويهـدف نظـام التحكم في الوصـول المعتمد على الـدور إلى جعل السياسـات الأمنية تعكـس العمليـات الفعلية للمنظمة. وكل فـرد في المنظمة ينبغـي أن يُمنح فقط الأدوار الضروريـة جداً لإتمام عمله بنجاح، وكل دور يجـب أن يحتوي فقط على الأذونات اللازمة لأداء المهـام المحددة. وبمـا أن نموذج نظام التحكم في الوصـول المعتمد على الدور يرتبط مباشرة بالوظائف الحقيقية للأفراد في المنظمة، يسـتطيع مسـؤولو أمن المعلومات العمل مباشرة مع مسـتخدمي النظام والمسـؤولين عن العمليات، وذلك بهدف تطوير السياسات التي سـيتم تطبيقها. وهذا الأمر مهم لأن مستخدمي النظام هم الخبراء في هذا الموضوع، فالمسـتخدمون يعرفون أذونات النظام اللازمة لوظيفة معينة، كما يعرفون المهام الوظيفية المرتبطة بوظيفة معينة.

سجل الوصول (Access Registry):

تُعد قاعدة بيانات سجل الوصول جوهر عملية إدارة الوصول حيث يوفر سجل الوصول لمسـؤولي الأمن رؤية موحدة لحسابات وأذونات الأفراد عبر المنظمة بأكملها. ويتم تدقيق

جميــع أنظمة تقنية المعلومات المرتبطة بنظام إدارة الوصول بشــكل دوري بهدف معرفة تغييرات الحسابات والأذونات وليتم بعد ذلك تحديث البيانات في سجل الوصول. وبالإضافة إلى ذلك يحتوي سجل الوصول على تطبيقات تقوم بتدقيق الوصول بشكل دوري. ويعمل تدقيق الوصول (Access audits) على تحديد مستوى الوصول الذي يستحقه كل فرد بناءً على البيانات المُقدمة من سـجل الشخص (Person Registry) والسياسات الأمنية الحالية. ومن خلال مقارنة نتائج تدقيق الوصــول (Access audits) مع بيانات الوصول المحفوظة في سجل الوصول، يستطيع مســؤول أمن المعلومات بسهولة تحديد مستوى الوصول الذي يجب أن يُضاف أو يُحذف وذلك لضمان امتثال النظام للسياسات الأمنية.

الخطــوة النهائية في عمليــة إدارة الوصول هي العمل على تغيــيرات الوصول المطلوبة عن طريق أنشطة الإرســال/ الاحتياط لجميع الخدمات والأنظمة المتأثرة. وتشمل أنشطة الاحتياط إنشاء حسابات أو إضافة أذونات لا يملكها الفرد أو حذف الحسابات أو الأذونات التي لم تعد هناك حاجة لها.[٢]،[٣].

معايير التدابير الاحتياطية

سابقاً كانت التطبيقات المستخدمة في إرسال أنشطة التدابير الاحتياطية متخصصة للغاية، كما كانت مكتوبة بشكل عام لاستهداف تطبيق أو خدمة واحدة فقط. لكن نظراً لأهميتها كان هناك توجه لإنشاء أُطر موحدة لإرسال البيانات الاحتياطية مثل «لغة ترميز خدمات التدابير الاحتياطية» (Service Provisioning Markup Language)[٢] (SPML) و«نظام إدارة الهوية عبر المجال» (System for Cross-Domain Identity Management)[٢] (SCIM). وتمت الموافقة على مواصفات نظام (SPML) في عام ٢٠٠٧، لكن استخدامه محدود، خاصة في المنظمات الكبيرة جداً، وذلك نظراً لتعقيدها. من ناحية أخرى يعد نظام (SCIM) جديداً نسبياً (تم إطلاق الإصدار الأول منه في شهر ديسمبر من عام ٢٠١١) وتسعى المنظمة جاهدة لتبسيطه. وما زال من السابق لأوانه معرفة ما إذا كان نظام (SCIM) سيصبح المعيار المستخدم على نطاق واسع، لكن يبدو أن هذا النظام حصل على دعم كبير من المزودين الرئيسين لخدمات الحوسبة السحابية.

وبمجرد انتهاء مسؤول النظام من عمليات إدارة الهوية وإدارة الوصول سيكون النظام جاهزاً لخدمة المســتخدمين. كما يحتاج النظام إلى توفير وسيلة للمســتخدمين لإثبات هوياتهم بحيث يمكن تقديم الامتيازات المناسبة لهم حيث تُمِكن آليات المصادقة المستخدمين من إثبات هوياتهم.

(2) https://www.oasis-open.org/committees/tc_home.php?wg_abbrev = provision

(3) http://www.simplecloud.info/

المصادقة (Authentication):

في شــبكات الحاســب الآلي، المصادقة هي العملية التي يقوم فيها المستخدم بإثبات أنه المالك للهوية التي يتم استخدامها. فعندما يقوم المستخدم بإدخال اسم المستخدم (والذي يســمى أيضاً أســاس الأمان) فإنه يحاول اســتخدام هوية للوصول إلى النظام. وللمصادقة على مســتخدم (أي التحقق أن المستخدم هو في الواقع صاحب الهوية) فإن الخطوة التالية الأكثر شــيوعاً هي أن نســأل عن بيانات الاعتماد. بيانات الاعتماد هي جزء (أو أجزاء) من المعلومات المُســتخدمة في التحقق من هوية المســتخدم. وتصنــف بيانات الاعتماد الأكثر شيوعاً إلى ثلاث فئات رئيسية:

- شيء تعرفه.
- شيء تملكه.
- شيء منك.

شيء تعرفه: كلمات المرور:

كلمة المرور هي أقدم وأبســط شــكل من أشــكال بيانات الاعتماد. وكلمة المرور هي سلسلة من الرموز السرية التي لا يعرفها سوى صاحب الهوية ويقوم باستخدامها للمصادقة عــلى الهويــة. فإذا قام الشــخص الذي يحاول الوصول إلى الحســاب بتوفــير كلمة المرور الصحيحة فإنه يُفترض أن هذا الشــخص هو صاحب الهوية ويتم منحه الوصول. وبلا شك أنك على دراية باســتخدام كلمات المرور. وتُستخدم كلمات المرور على نطاق واسع لأنها لا تحتــاج إلى أجهزة ولا تحتاج إلى برمجيات لتطبيقها. وعلى الرغم من أن اســتخدام كلمات السر يُعد الأكثر شــيوعاً من بين بيانات الاعتماد الأخرى، إلا أننا رأينا سابقاً أن هناك العديد من المســائل المتعلقة بأمــن كلمات المرور بما في ذلك كلمات المــرور الضعيفة. وأيضاً فإن المهاجمين يستخدمون طريقتين شائعتين لتخمين كلمات المرور[٤]:

(٤) وللاطلاع على تقرير سهل القراءة عن حالة السوق، انظر الرابط التالي،

http://www.dailymail.co.uk/sciencetech/article-2331984/Think-strong-password-Hackers-crack-16-character-passwords-hour.html#ixzz2UcKeZwyW (accessed 042013/4/)

- هجمات القاموس (Dictionary attacks): تجريب الآلاف من كلمات المرور وذلك من قواميس ضخمة لكلمات المرور والكلمات الشائعة من لغات متعددة.
- هجمات القوة الغاشـمة (Brute-force attacks): مزج الرموز عشـوائياً وتجريبها حتى يتم تخمين كلمة المرور حيث يتم تجريب كل مزيج ممكن من الرموز.

وتسـتطيع هجمات القاموس تخمين كلمات المرور الشائعة بسرعة، لكنها ليست فعالة ضـد كلمات المرور التـي تحتوي على أرقام ورمـوز متعددة بالإضافـة إلى الحروف. لكن هجمات القوة الغاشمة، من ناحية أخرى، تستطيع تخمين أي كلمة مرور عندما يكون لديها الوقـت الكافي لذلـك. وللتغلب على نقطة الضعف هذه، تقـوم معظم المنظمات بتشريع سياسات تفرض كلمات مرور قوية. وفيما يلي بعض من القواعد النموذجية المستخدمة:

- يجب أن تتكون كلمة المرور من ثمانية رموز أو أكثر.
- يجب أن تحتوي كلمة المرور على رقم، وحرف صغير، وحرف كبير، ورمز خاص.
- يجب ألا تحتوي كلمة المرور على كلمة من القاموس.

مقياس عشوائية كلمة المرور (Password entropy):

لسوء الحظ فإن تلك القواعد تولد كلمات مرور يصعب تذكرها، ولكن لا تؤدي بالضرورة إلى كلمات مرور قوية. ففي عام ٢٠٠٦ أصدر المعهد الوطني للمعايير والتكنولوجيا (National Institute of Standard and Technology) منشوراً خاصاً (٨٠٠-٦٣)[٥] يُقدم تعريفاً حسابياً لقوة كلمة المرور اعتماداً على مقياس عشوائية (entropy)[٦] كلمة المرور. ويسمح لك مقياس العشوائية بمعرفة الوقت المستغرق للمهاجم لتخمين كلمة مرور معينة باستخدام هجمات القوة الغاشمة. على سبيل المثال، كلمة المرور التالية (d٣nT١ty!) تُعد كلمة مرور قوية لأنها تلبي جميع القواعد النموذجية التي تم ذكرها أعلاه. واتضح أن كلمة المرور هذه تحتوي على ٢٥ بتاً من مقياس العشوائية والتي تمثل ٢٢٥ كلمة مرور محتملة (٣٣ مليون). وفي المتوسط فإن المهاجم يقوم بمحاولة أكثر من (١٦ مليون) كلمة مرور لتخمين القيمة الصحيحة. وبمعدل ١٠٠٠ محاولة في الثانية فإن المهاجم سيستغرق فقط ٤ ساعات لتخمين كلمة المرور. لكن عند استخدامك ٣-٤ كلمات شائعة، بدلاً من استخدام كلمة واحدة، باعتبارها عبارة المرور مثل «ورقة مقص حجر» تكون رفعت مقياس العشوائية إلى ٢٤١ والذي سيزيد من الوقت المطلوب لتخمين كلمة المرور إلى أكثر من ٨ سنوات.

وكما ترى فإن كلمة مرور ذات المقياس العشوائي العالي ستكون أكثر مقاومة لهجمات القوة الغاشمة[٧].

---

(5) http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf

(٦) مقياس للفوضى والعشوائية في النظام المغلق (Houghton Mufflin Harcourt eReference)

(٧) انظر مقالاً عن هذا الموضوع، Bruce Schneier, «Passwords are not broken, but how we choose them (2013/18/sure is,» http://www.schneier.com/essay-246.html(accessed 07

شيء تملكه: القطع الرمزية:

بدلاً من إســناد المصادقة إلى سر يعرفه المُستخدم ويمكن أن يشترك في معرفته (عمداً أو غير ذلك) شــخص آخر، فإن القطع الرمزية عبارة عــن المكونات المادية (أو في حالة القطع الرمزيــة البرمجية المخزنة في شيء مادي) التي يجب تقديمها لإثبات هوية المســتخدم. وفي جميــع الحــالات تقريباً فإن القطع الرمزيــة ترافق كلمات المــرور («شيء تملكه» و «شيء تعرفــه») مما يؤدي إلى إنشــاء نظام توثيق ثنــائي العوامل. ويُعد نظــام (التوثيق الثنائي العوامل) وســيلة بســيطة نسبياً لإنشــاء درجة عالية من الثقة في هوية الفرد الذي يحاول الوصول إلى النظام. وقد استخدمت المؤسسات المالية نظام التوثيق الثنائي العوامل (بطاقة الــصراف الآلي والرقم السري) لعقود من الزمــن، وكذلك الشركات الكبيرة. لكن ومع زيادة حالات الانتحال الإلكتروني وغيرها من هجمات كلمات المرور في الســنوات الأخيرة، توجهت العديد من المنظمات لإضافة عامل إضافي لنظام المصادقة الحالي.

أما البطاقات الذكية فهي عبارة عن قطع رمزية في حجم البطاقة الائتمانية تقوم بحفظ رقم الهوية، والذي يحدد البطاقة بشكل فريد، أو تحتوي البطاقة الذكية على ذاكرة صغيرة تحفظ توثيقاً رقمياً يُحدد المســتخدم نفســه. ويتم استخدام البطاقات الذكية في مجموعة واســعة من التطبيقات، بدءاً من بطاقات (SIM) الهاتفية داخل كل هاتف محمول وصولاً إلى بطاقــات الوصــول المُســتخدمة في الوصول المــادي لتأمين مناطق المنشــآت الحكومية والعسكرية. وبديلاً للمصادقة المستندة إلى التوثيق، يمكن تحميل التوثيق مباشرة في قرص يو إس بي (USB thumb drive) (الشــكل ٨-٣). وتســاعد القطع الرمزية المُعتمِدة على التوثيــق باســتخدام قرص يو إس بي (USB) على الاســتغناء عن قــارئ البطاقة الذكية كما تساعد على تأمين الحفظ الداخلي من خلال استخدام كل من التوثيق وكلمة المرور.

ومن عيوب القطــع الرمزية المعتمدة على البطاقات الذكية، وكذلك من عيوب التوثيق باســتخدام قرص يو إس بي (USB) أن المســتخدم يجب أن يكون لديه وصول مادي لمنفذ يــو إس بي (USB) أو يكون لديــه قارئ بطاقة ذكية موصول بالنظــام. وهذا ليس ممكناً دائماً خاصة عند اســتخدام الأجهزة المحمولة أو عند تســجيل الدخول من مختبر حاســب آلي مفتــوح الاســتخدام أو مقهى للإنترنــت. وفي هذه البيئات فإن القطــع الرمزية التي لا

تحتاج إلى اتصال مباشر بجهاز الحاســب الآلي تكون مطلوبة. وبإمكان قطع رمزية بحجم سلســلة المفاتيح مــن شركة (RSA) وشركة (Vasco) التعامل مع هذه المشــكلة من خلال توليد سلســلة من الأرقام التي يتم عرضها على شاشة (LCD) صغيرة في الجزء الأمامي من القطعة الرمزية. وبعد ذلك يتم إدخال سلسلة الأرقام من قبل المستخدم ككلمة مرور لمرة واحدة (one-time password)، وهي عبارة عن كلمة المرور يمكن استخدامها لمرة واحدة فقــط وعادة تكون صالحة لفترة محدودة فقط. وتُعد القطع الرمزية التي من هذا القبيل (الشــكل ٨-٤) شائعة الاستخدام منذ ســنوات عديدة في القطاع الخاص والقطاع الحكومي لأنها سهلة التطبيق نسبياً، ولا تتطلب قارئاً خاصاً أو غيرها من الملحقات لتكون متصلة بكل جهاز حاسب آلي في المنظمة، كما يمكن استخدامها بسهولة في أجهزة الحاسب الآلي المكتبية أو المحمولة.

الشكل (٨-٣): بطاقة ذكية في قارئ بطاقة متصل بمنفذ يو إس بي (USB)





الشكل (٨-٤): قطعة رمزية (Token)



وتقــوم هذه الأنواع من القطع الرمزية باســتحداث كلمة مــرور لمرة واحدة من خلال أساليب تعتمد على الوقت أو أساليب تعتمد على التسلسل.

- تعمل القطــع الرمزية التي تعتمد على الوقت على اســتحداث كلمة مرور جديدة خلال فترة زمنية محددة، عادة تكون ٣٠ أو ٦٠ ثانية.
- أمــا القطع الرمزيــة التي تعتمد على التسلســل فتســتخدم خوارزميــات معقدة لاستحداث سلسلة من كلمات مرور لا يمكن تخمينها بناءً على كلمات المرور السابقة في هذه السلسلة.

وبغض النظر عن النوع المستخدم، يتم تسجيل القطعة الرمزية في خادم التوثيق قبل أن تُعطى للمستخدم، مما يؤدي إلى إعطائها قيمة مبدئية لبدء خوارزمية تعتمد على التسلسل أو إلى مزامنة الساعة الداخلية لبدء الأسلوب المُعتمِد على الوقت.

وبالإضافــة إلى القطع الرمزية فإن موردي الأجهزة الأمنية مثل شركة (RSA) تُقدم قطع رمزيــة برمجيــة (software tokens)، وهي عبارة عن تطبيقــات للهاتف المحمول تعمل بنفس طريقة القطع الرمزية لكن لا تتطلب من المستخدم أن يحمل جهاز منفصل. ولأنها لا تنطوي على تقديم جهاز فعلي فإن هذه القطع الرمزية البرمجية لها فائدة إضافية تتمثل في الانتشار السريع والبسيط – من خلال تثبيت التطبيق. وبمجرد تثبيت التطبيق فإن القطع

الرمزيـــة البرمجيـــة تعمل تماماً مثل القطع الرمزية الماديـــة المتنوعة - يقوم التطبيق بتوليد كلمة مرور تســتخدم لمرة واحدة، والتي يمكن بعد ذلك دمجها مع كلمة مرور المســتخدم لتحقيــق مصادقة النظام. وتُعد أداة مصادقــة جوجل (Google Authenticator) قطعة رمزية برمجية للمصادقة الثنائية العوامل لحســابات جوجل، وذلك في الهواتف الذكية التي تعمل بنظام الآي أو إس (iOS) ونظام الآندرويد (Android)[8].

وبالإضافــة إلى تطبيقات القطع الرمزية البرمجية فإن القدرات المميزة للأجهزة المحمولة الحديثــة زادت من عدد الخيــارات المتاحة للمصادقة الثنائية العوامل. فالرســائل النصية القصيرة (SMS) تُعد طريقة مبسطة لتوفير عامل إضافي للمصادقة حيث يقوم المستخدمون أثناء إعداد حســاباتهم بتســجيل أرقام هواتفهم المحمولة في خدمة المصادقة. وبعد ذلك عندما يحاول المستخدم المصادقة، يتم إرسال رمز المرور في رسالة قصيرة إلى هاتفه المحمول. ثم يقوم المســتخدم بإدخال الرمز لإثبات أن الهاتف المحمول والمســجل مســبقاً لا يزال في حوزته. وأحد عيوب اســتخدام الرســائل القصيرة وســيلة لاعتماد بيانات المصادقة هو أن العديد من شركات الهاتف المحمول تأخذ رسوماً على كل رسالة.

وتُقدِم شركة (tiQR) (http://tiqr.org) مثالاً عن نهج جديد للمصادقة وذلك بالاستفادة مــن الميــزات الموجودة في الهواتف الذكية. فعند تســجيل الدخــول إلى موقع محمي من شركة (tiQR)، يتم عرض عبارة مرور مشفرة للمستخدم على شكل رمز للاستجابة السريعة (Quick Response code). وبعــد ذلــك يقوم المســتخدم بأخذ صورة لرمز الاســتجابة السريعة باســتخدام تطبيق (tiQR) الموجود في الجهاز الذكي للمستخدم (وتطبيق (tiQR) متوفر على أجهزة أندرويد (Android) وأجهزة آي أو إس (iOS) وقت إعداد هذا الكتاب). ثم يقوم المســتخدم بإدخال كلمة المرور في تطبيق (tiQR) ويرسلها إلى خادم المصادقة مع عبارة المرور التي تم فك شفرتها. ويقوم خادم المصادقة بالتحقق من كلمة مرور المستخدم ومن عبارة المرور للتأكد من هوية المستخدم.

شيء منك: القياسات الحيوية (biometrics):

تُعد القطع الرمزية والقطع الرمزية البرمجية وســيلة رائعــة لإضافة عامل إضافي لزيادة الأمــن، ولكــن مثل أي شيء مــادي فإن القطــع الرمزية يمكن أن تضيــع أو تسرق ومن ثم

(8) http://googleonlinesecurity.blogspot.com/2012/03/improved-google-authenticator-app-to.html

تُســتخدم من قبل المهاجمين لانتحال شخصية المستخدمين. كيف يمكننا التأكد بأن الشخص الــذي يحاول الوصول إلى النظام هو بالتأكيد الشــخص صاحب الهويــة؟ الأجهزة الحيوية تحلل الفروق الدقيقة في بعض المواصفات الجســدية أو الســلوكية، مثل بصمات الأصابع أو نمط الأوعية الدموية في العين، وذلك لتحديد هوية الفرد. وبشكل عام فإن الأجهزة الحيوية تعمل من خلال مقارنة بين بيانات القياســات الحيوية التي يتم أخذها من الشــخص وبين نســخة من بيانات القياسات الحيوية للشخص والتي تم أخذها سابقاً أثناء عملية التسجيل. وإذا كانت بيانات القياســات الحيوية للشــخص الــذي يحاول الوصــول إلى النظام تطابق البيانات المحفوظة في النظام، فإنه يُفترض بأنه نفس الشخص وتكون عملية المصادقة ناجحة.

ويطلق على الفروق المادية التي يمكن ملاحظتها بين الناس بالعلامات الحيوية. وهناك العديــد من العلامات التي يمكن اســتخدامها، ولكن يتم تحديد مدى ملاءمة العلامات من خلال العديد من العوامل، بما في ذلك[٩]:

- العمومية: يجب أن تكون السمة أو الصفة لدى كل شخص.
- التفرد: لا يوجد شخصان لهما الصفة نفسها.
- الدوام: يجب ألا تتغير الصفة مع مرور الوقت.
- التحصيل: يجب أن تكون الصفة قابلة للقياس كمياً.
- الأداء: يجب أن يتم الحصول على قياس دقيق من خلال موارد معقولة.
- القبول: استعداد المستخدمين لقبول قياس الصفة.
- التلاعب: صعوبة تقليد صفات شخص آخر[١٠].

(9) Jain, A.K., Bolle, R., Pankanti, S., eds. Biometrics: Personal Identification in Networked Society. Kluwer Academic Publications, 1999

(١٠) في شهر يونيو من عام ٢٠١٣، كان موضوع القياسات الحيوية في الإعلام عندما حكمت المحكمة العليا في الولايات المتحدة بشرعية جمع القياسات الحيوية للتعرف على من يُقبض عليهم، واستخدام تلك القياسات في الكشف عن جرائم أخرى ليست ذات صلة بالجريمة الأساسية، Maryland vs. King, http://www.scotusblog.com/case-files/cases/maryland-v-king/ (Accessed 10/11/13)

بصمات الأصابع:

تُعد بصمات الأصابع أكثر العلامات الحيوية المعروفة والمستخدمة حتى الآن. وتتكون بصمات الأصابع من نمط فريد من النتوءات على الأصابع، أو على راحة اليد البشرية والتي تُعد فريدة من نوعها أيضاً - خلال أكثر من ١٠٠ عام من التحقيق في مسرح الجريمة، وفي أكثر من ملايين من بصمات الأصابع، لم يتم العثور على الإطلاق على اثنين لديهم بصمات أصابع متطابقة.

وفي السابق كانت تكنولوجيا مسح بصمات الأصابع شائعة الاستخدام فقط في التطبيقات التي تتطلب أماناً عالياً، لكن ومع انخفاض أسعار تكنولوجيا المسح وانخفاض تعقيدها أصبحت ماسحات بصمات الأصابع جزءاً من الأجهزة الموحدة في أجهزة الحاسب الآلي المكتبية المصممة لاستخدام قطاع الأعمال. وتعتمد (ماسحات بصمات الأصابع) إما على مجسات ضوئية في شكل كاميرا صغيرة تأخذ صوراً رقمية للإصبع، أو على ماسحات ضوئية بالسعة (capactive scanners) والتي تولد صورة من إصبع المستخدم باستخدام التيار الكهربائي. وبدلاً من مقارنة كامل بصمة الإصبع، يقوم برنامج المسح الضوئي بمقارنة شكل ومكان العديد من ميزات البصمة الفريدة (التفصيلات) (الشكل ٨-٥). وعن طريق مطابقة التفصيلات بين بصمتي الأصابع، يستطيع البرنامج حساب احتمال تطابق البصمتين. وهذا النوع من المطابقة الاحتمالية يمنع العوامل البيئية (الإضاءة، البقع الموجودة على الكاميرا، وغيرها) من التأثير على نتيجة تطابق بصمات الأصابع. ومع ذلك فإنها تُعد نقطة ضعف في مصادقة القياسات الحيوية. ولا يحتاج المهاجم للحصول على تطابق تام للبصمة من أجل انتحال الشخص المستهدف بل يكفي أن يقوم المهاجم بنسخ ما يكفي من «التفصيلات» من أجل إقناع الماسح الضوئي بأنه الشخص الصحيح «المحتمل». وعلى الرغم من أنه تم نشر الهجمات الناجحة ضد ماسحات بصمات الأصابع[11] إلا أنها ستظل التقنية الآمنة عموماً والتقنية الأكثر استخداماً في تحديد هوية القياسات الحيوية لسنوات قادمة.

مسح قزحية وشبكية العين:

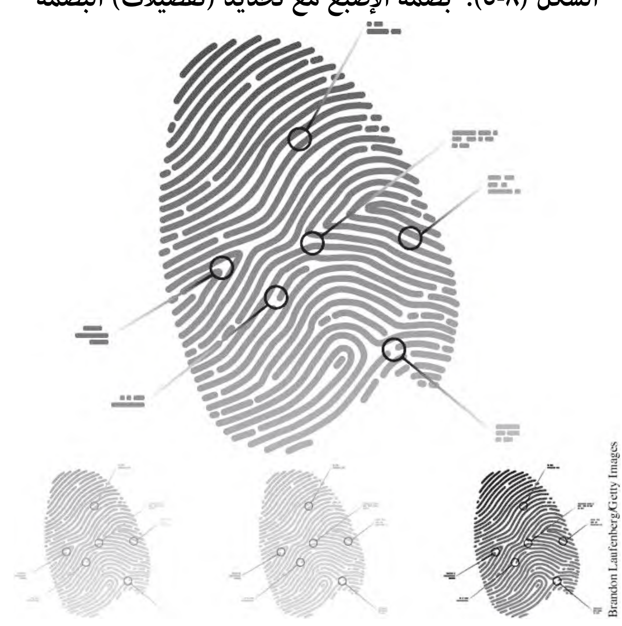
تسجل الماسحات الضوئية لشبكية العين النمط الفريد من الأوعية الدموية الموجودة في

(11) Matsumoto, T. et al. Impact of Artificial «Gummy» Fingers on Fingerprint Systems. International Society of Optics, 2002

الجزء الخلفي من العين. وبالإضافة إلى شبكية العين، تحتوي العين على سمة تحديد فريدة أخـرى هي القزحية. والقزحية هـي الهيكل الدائري الذي يحيط بؤبؤ العين ويعطي العين لونها. وبشـكل مشـابه لبصمات الأصابع فإن هذه الهياكل فريدة من نوعها لكل شـخص ويمكن اسـتخدامها للمصادقة. ولفترة طويلة كان مسـح القزحية والشبكية جزءاً من أفلام التجسـس - الدخول إلى قاعدة سرية أو مسـح العين للتحقق مـن الهوية من خلال نظام أمنيٍ. أما في الحياة العملية فإن هذه الأنظمة تُسـتخدم لحماية المناطق التي تتطلب أمناً عالياً مثل وزارة الدفاع أو مناطق عادية مثل الصالة الرياضية المحلية.

وقد اسـتخدمت الماسـحات الضوئية لشـبكية العين في أعلى المناطق الأمنية لسـنوات عديدة. وبالنسـبة للمسـتخدم فإن مسح شـبكية العين مشـابه إلى حد كبير إلى الاختبار الـذي يُجرى في مكتب طبيب العيون حيث يتم النظر إلى عدسـة، ويتم التركيز على نقطة من الضوء لعدة ثوان، في حين يلتقط الماسـح الضوئي صورة لشـبيكة العين، ثم يقوم الماسح بمعالجة البيانات. ويعد مسح شبكة العين دقيقاً للغاية لكنه لا يُعد مقبولاً للاستخدام العام لأنه توسعي أكثر من التقنيات الأخرى، كما أنه أبطأ من البدائل الأخرى.

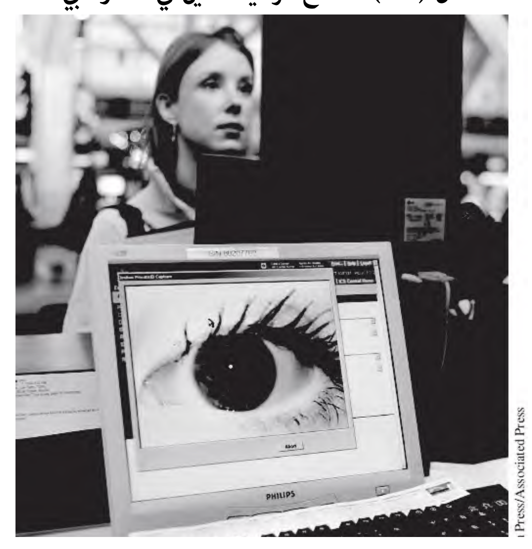
الشكل (٨-٥): بصمة الإصبع مع تحديد (تفصيلات) البصمة



وعلى عكس المســح الضوئي لشــبيكة العين فإن مســح قزحية العين سريــع وغير مؤلم. وماســح قزحية العين هو عبارة عن كاميرا رقمية عادية (صور ثابتة أو فيديو) مزودة بفلتر أشــعة تحت الحمراء (infrared) والذي يسمح بالتقاط صورة محسنة للقزحية. وإن كان مســح قزحية العين ليس دقيقاً كمسح شــبكية العين إلا أنه يُستخدم في العديد التطبيقات بسبب سهولة الاستخدام. ويُعد مسح قزحية العين مشابهاً جداً لأخذ الصور بالكاميرا حيث لا يتطلب مســح القزحية أن يكون المســتخدم على مقربة من الماسح الضوئي (بحدود أمتار قليلة) أو يبقى ثابتاً لفترة طويلة من الزمن، وذلك لأن الصور يتم التقاطها بشكل فوري.

وفي عام ٢٠٠١ بدأت وزارة الداخلية في دولة الإمارات العربية المتحدة برنامجاً للمســح الضــوئي لجميع الرعايا الأجانب الذين يدخلون البلاد، وذلك بحثاً عن الأشــخاص الذين تم طردهم ســابقاً من البلاد بســبب انتهاكات تصاريح العمل (الشكل ٨-٦). ويحتوي النظام عــلى ملايين من الهويات كما يقوم بمليارات من عمليــات البحث يومياً. وحتى الآن تمكن النظام من القبض على أكثر من ١٠ آلاف شــخص كانوا يحاولون معاودة الدخول إلى البلاد بوثائق سفر مزورة[١٢].

شكل (٨-٦): مسح قزحية العين في مطار دبي



(12)Daugman, J. Encyclopedia of Biometrics. Springer, 2010

وقـد بدأ مسـح قزحية العين بالانتقال مـن المنظمات الحكومية الكبـيرة إلى تطبيقات منظـمات القطاع الخاص. على سـبيل المثال، فقد زودت شركة نـوادي اللياقة (Equinox Fitness Clubs) مواقعها الخمسـة عشر بماسحات ضوئية لقزحية العين بدلاً من ماسحات البطاقة التقليدية المُسـتخدمة في نوادي اللياقة البدنية الأخرى. وقد سـمحت ماسـحات قزحيـة العـين لأعضاء «كبار الشـخصيات» (VIP) بالوصول إلى الخدمـات الحصرية دون الحاجة إلى حمل بطاقة أو الحاجة إلى تذكر الرقم السري[١٣].

مشكلات نظام القياسات الحيوية:

تُعد أنظمة القياسـات الحيوية شـكلاً آمناً للغاية لتحقيق المصادقـة الثنائية العوامل، كما يمكن أن توفر هذه الأنظمة درجة عالية من الثقة في هوية المسـتخدم، لكن أداء هذه الأنظمة يعد أحد العقبات. فإذا قام المهاجم بسرقة كلمة مرور المستخدم أو القطع الرمزية الأمنية الخاصة به فإنه يتم إزالة التهديد بمجرد إصدار كلمة مرور جديدة أو إصدار قطعة رمزيـة جديـدة. وهذا ليس ممكناً عنـد التعامل مع بيانات القياسـات الحيوية. وبحكم طبيعتهـا فإن العلامات الحيوية دائمة - لا يمكن إصـدار بصمات أصابع جديدة في حال تم اخـتراق بيانات بصـمات الأصابع. ومن ثم فإن هذه العلامة الحيوية لا يمكن اسـتخدامها كعامـل مصادقة موثوق به. وهنا يجب إما ترقية نظام بصمات الأصابع لإزالة الخلل الذي يسمح للمهاجمين بتقليد المستخدم الحقيقي، أو استبدال النظام بأكمله من خلال استخدام علامة حيوية مختلفة[١٤].

> تبدو القياسات الحيوية حديثة لكنها من أقدم أشكال تحديد الهوية. فالنمور تتعرف على بعضها من خلال رائحتها. وطيور البطريق تتعرف على بعضها من خلال النداءات. والبشر يتعرفون على بعضهم من خلال النظرات المباشرة، والأصوات على الهاتف، والتوقيعات على العقود، والصور على رخص القيادة. وقد استُخدمت بصمات الأصابع للتعرف على الأشخاص في مسرح الجريمة لأكثر من ١٠٠ عام. والجديد الآن في القياسات الحيوية هو قيام أجهزة الحاسب الآلي بعملية التعرف: بصمات الإبهام، ومسح شبكية العين، وتخطيط الصوت، وأنماط الكتابة[١٤].

(13) «Equinox Fitness Clubs Case Study.» IRIS In Action. IRISID. Web. 15 May 2013

(14) Bruce Schneier, Crypto-gram, January 15, 2009

تسجيل الدخول الأحادي (Single sign-on):

عند التحقق من هوية المســتخدم فإنه يُمنح حق الوصول إلى النظام أو إلى التطبيق. وإذا كانت هذه المصادقة على الحســاب المحلي، مثل تسجيل الدخول إلى نظام ويندوز عند تشغيل جهاز الحاسب الآلي الخاص بك، فإن عملية المصادقة تكون مكتملة. ويقوم نظام التشــغيل بإعلام جميع البرامج في جهاز الحاســب الآلي بهويتك ومن ثم لا حاجة للقيــام بالمصادقة مرة أخرى. لكن ما الذي يحدث إذا كان التطبيق الذي تريد الوصول إليه موجوداً على نظام آخر؟ كيف يمكنك أن تُعرف نفسك إلى التطبيق البعيد؟ ومثال عــلى ذلــك، الوصول إلى معلومات مادة دراســية موجــودة على (نظــام إدارة التعلم) (learning management system) مثل نظام بلاكبورد (Blackboard).

بإمكانك تكرار عملية المصادقة وتزويد النظام باســم المستخدم وكلمة المرور وأي عامل آخر (مثــل القطع الرمزية، والقياســات الحيوية، وغيرها) المطلوبــة في البيئة الخاصة بك. وهذا ســيؤدي الغرض لكن سرعان ما يُصبح ذلك مملاً خصوصاً إذا كنت ترغب في الوصول إلى العديــد مــن الأنظمة. وما نحتاج إليه هو وســيلة تســاعد على تســجيل الدخول مرة واحــدة ومن ثم الوصول إلى جميع التطبيقــات المتصلة دون المُطالبة ببيانات الاعتماد مرة أخرى. ويُشــار إلى هذا النظام بـ «تســجيل الدخول الأحادي» (SSO) (single sign-on) ويمكن تحقيقه بعدد من الطرق. ويُقصد بـ «تســجيل الدخول الأحادي» هو التقنية التي تســمح للمستخدم بتسجيل الدخول مرة واحدة ومن ثم الوصول إلى جميع الموارد المُصرح للمستخدم الوصول إليها.

وعموماً فإن مســؤول النظام في بيئة «تســجيل الدخول الأحادي» يقوم بإنشــاء كلمة مرور للمســتخدم لكل مَورِد يُســمح للمســتخدم بالوصول إليه بحيث تكون كلمة المرور قوية وفريدة، كما يقوم مسؤول النظام بتغيير كلمات المرور التابعة للموارد الفردية بشكل منتظم كما هو محدد من قِبل سياســة كلمات المرور التابعة للمنظمة. والمُستخدم النهائي ليــس عــلى علم بأي من كلمات المــرور التابعة للموارد الفردية. وبــدلاً من ذلك يتم منح المســتخدم كلمة مرور واحدة يقوم بإدخالها للوصول إلى المــوارد التي يتم التحكم بها من خلال تقنية «تسجيل الدخول الأحادي».

ويتم تنفيذ تقنية «تسجيل الدخول الأحادي» عادة من خلال استخدام مستودع مركزي واحــد للمصادقــة المُعتمدة على كلمات المرور. وبمجرد قيام المســتخدم بالمصادقة في هذا المستودع المركزي يقوم النظام بالبحث عن الموارد المصرح للمستخدم الوصول إليها. وعند محاول المستخدم الوصول لأي من هذه الموارد فإن نظام «تسجيل الدخول الأحادي» يعمل على توفير كلمة المرور الخاصة بالمَورد نيابة عن المســتخدم. وأصبح اســتخدام «تســجيل الدخول الأحادي» شائعاً بازدياد في المنظمات الكبيرة مثل الجامعات والمصارف.

مزايا وعيوب نظام تسجيل الدخول الأحادي:

قبل الحديث عن التقنيات المختلفة لـ «تســجيل الدخول الأحــادي»، دعنا نُلقي نظرة على مزايا وعيوب نشر «تســجيل الدخول الأحادي» في النظــام. هناك العديد من الفوائد الرئيســية التي يقوم «تســجيل الدخول الأحادي» بتوفيرها مباشرة لكل من المســتخدمين ومسؤولي النظام:

- تجربة أفضل للمستخدم: فلا أحد يُحب إدخال بيانات الاعتماد عدة مرات.
- تُحفــظ بيانات الاعتماد بشــكل سري: بحيث يكون المســتخدم وخادم «تســجيل الدخول الأحادي» فقط لديهم إمكانية الوصول إلى بيانات اعتماد المستخدم. وهذا يُلغي إمكانية وصول المهاجم لكلمة المرور من خلال خدمة مُخترقة.
- تنفيذ سهل للمصادقة الثنائية العوامل بدلاً من تحديث جميع الخدمات التي تدعم المصادقة من خلال القطع الرمزية وبيانات القياســات الحيوية، فإن نظام «تسجيل الدخول الأحادي» فقط يحتاج إلى التحديث.
- أقل حيرة: لا يحتاج المســتخدمون إلى تذكر حســابات متعددة بأسماء مستخدمين وكلمات مرور مختلفة.
- مكالمات أقل لمكتب المســاعدة الفنية: على الأغلب فإن المســتخدمين ســيتذكرون كلمات المرور التابعة لهم.
- كلمات مرور قوية: بما أن المُستخدم يحتاج لتذكر كلمة مرور واحدة فقط فإنه من الممكن أن تكون كلمة المرور أكثر تعقيداً.
- تدقيق مركزي: يتم تأمين جميع المصادقات ويمكن رصدها في مكان واحد.

وبشــكل عام فإن تطبيق تقنية «تســجيل الدخول الأحادي» تطور من مســتوى الأمن ومن خبرة المستخدم، لكن هذه التقنية لا تخلو من العيوب:

- اختراق بيانات الاعتماد يمثل خطراً كبيراً - فاختراق حســاب واحد يؤدي إلى الوصول إلى العديد من الأنظمة أو التطبيقات.
- هجمات الانتحال - وجود صفحة تســجيل واحدة يمثل هدفاً جذاباً للمخادعين حيث يســتطيع هــؤلاء المخادعون من نســخ لغــة ترميز النصوص التشــعبية (HTML) «HyperText Markup Language» الخاصة بصفحة تســجيل الدخول التابعة لك مما يسهل سقوط المستخدمين في هذه الخدعة.
- يمثــل نظام «تســجيل الدخــول الأحادي» نقطة عطــل مفــردة (single point of failure). فــإذا لم يكن هــذا النظام متوفراً لا يمكن لأحــد المصادقة على أي نظام. وتعطل هذا المســتودع سيؤدي للإضرار ليس فقط بخصوصية وتكامل جميع كلمات المرور في المســتودع، بل سيضر أيضاً بجاهزية جميع الأنظمة التي يتحكم فيها هذا المستودع.
- إضافة أي نوع من «تســجيل الدخول الأحادي» ســيزيد من تعقيد النظام بأكمله. وكلما كان الحل أكثر تعقيداً، زادت احتمالية حدوث الأخطاء.

مزامنة كلمات المرور:

وبالإضافة إلى «تسجيل الدخول الأحادي»، تقوم بعض المنظمات بتوظيف نظام مصادقة لمزامنــة كلمات المــرور (password synchronization). وتهــدف خدمة مزامنة كلمات المرور لضمان أن المســتخدم لديه نفس اســم المســتخدم وكلمة المرور في جميع الأنظمة. وبعكس «تســجيل الدخول الأحادي» فإن المســتخدم لمزامنة كلــمات المرور يقوم بإدخال بيانــات الاعتــماد عند الدخول لكل نظام. ويؤدي تغيير كلمة المرور في نظام واحد إلى نشر هذا التغيير إلى الموارد الأخرى. وهذا يقلل من حيرة المســتخدم كما قد يقلل من المكالمات الهاتفية لمكتب الدعم الفني والتي تهدف لإعادة تعيين كلمات المرور.

وعلى عكس «تســجيل الدخــول الأحادي» فــإن مزامنة كلمات المــرور لا تحتوي على مســتودع مركزي لكلمات المرور. وبدلاً من ذلك، يقوم كل نظام مزامنة بحفظ نســخة من كلمة مرور المســتخدم ويقوم المســتخدم مباشرة بالمصادقة على كل نظام. والفائدة التي تعود على المســتخدم هي أن هناك كلمة واحدة فقط ليتذكرها. وتُستخدم مزامنة كلمات المــرور عادة عند دمج عدة أنــواع مختلفة من الأنظمة معاً. على ســبيل المثال، يجب أن يكون المســتخدم قادراً على الوصول إلى تطبيق على شــبكة الإنترنت، والوصول إلى تطبيق يعمل على الحاســوب الرئيسي، والوصول أيضاً إلى قاعدة بيانات الحسابات وذلك باستخدام بيانات الاعتماد نفسها.

وبما أن مزامنة كلمات المرور تحتاج إلى متطلبات قليلة للتنفيذ، فإنها عموماً أقل تكلفة من «تسجيل الدخول الأحادي». ومع ذلك فإن مزامنة كلمات المرور لها مشكلاتها الخاصة. ولأن كلمة المرور نفســها تُســتخدم في العديد من الموارد فإن اخــتراق أي من هذه الموارد ســيؤدي إلى اختراق جميع المــوارد المتزامنة مع المورد المُختَرَق. وإذا تم اســتخدام مزامنة كلــمات المرور مع موارد ذات متطلبــات أمنية مختلفة، فإن المهاجم يســتطيع حينها من اخــتراق الموارد الأقل أمنــاً للوصول إلى الموارد الأكثر أمناً والتي مــن المتوقع أن تكون ذات قيمة عالية.

الدليل النشط وبروتوكول كيربيروس (Active directory and Kerberos):

في شــبكات مايكروســوفت ويندوز، يُمثل الدليل النشــط (Active directory) هيكل «تســجيل الدخول الأحادي». ويقوم الدليل النشــط (Active directory) بدمج خدمات الشبكات بما في ذلك «نظام اسم المجال» (DNS) و«البروتوكول الخفيف للوصول إلى الدليل» (LDAP) مع بروتوكول كيربــيروس (Kerberos). وبروتوكول كيربيروس (Kerberos) هو بروتوكول مصادقة يســمح للأجهزة الطرفية الموجودة في شبكة غير آمنة للتعريف بأنفسهم ولتعرف بعضهم على بعض وذلك بشــكل آمن باستخدام القطع الرمزية. كما أن بروتوكول كيربيروس (Kerberos) بروتوكول مصادقة شائع الاستخدام، ويُعد أساساً لتقنيات المصادقة الأخــرى. وتم تطوير مــشروع بروتوكول كيربــيروس (Kerberos) في الثمانينيات من قبل

باحثين في معهد ماساتشوستس للتكنولوجيا (MIT) وتم إتاحته للجمهور في عام ١٩٩٣ [١٥] . ويعمل بروتوكول كيربــيروس (Kerberos) على توفير درجة عالية جداً من الثقة في الهوية المقدمة للتطبيق المحمي من خلال بناء علاقة موثوقة اســتناداً إلى مفاتيح التشفير المشتركة بين خادم المصادقة، والتطبيق المحمي، والعميل.

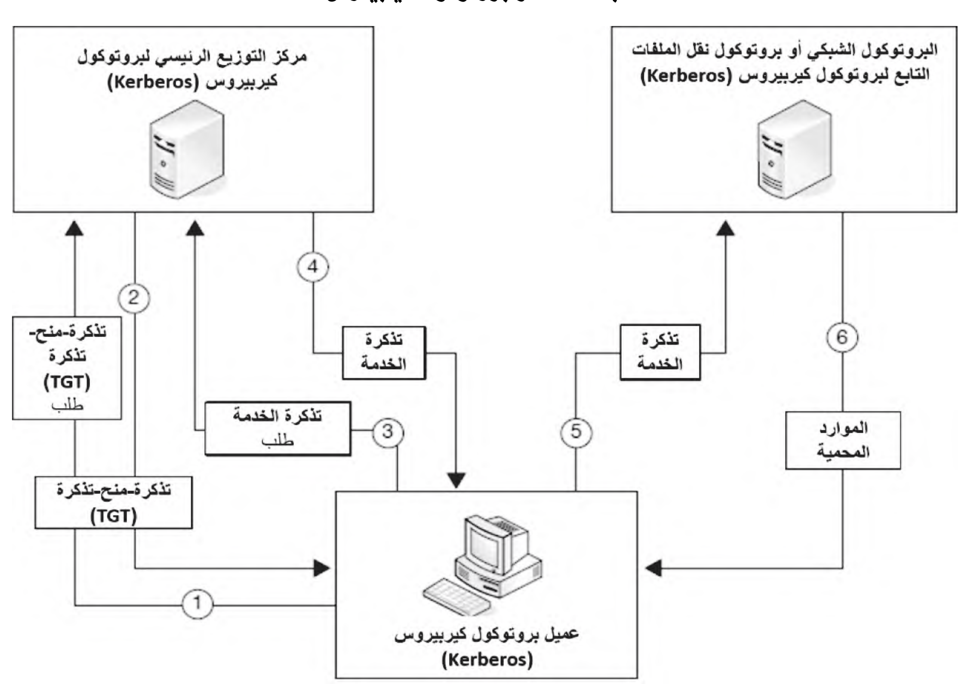
وفي عمل روتيني لبروتوكول كيربيروس (Kerberos)، قد يرغب المُســتخدم في استخدام خدمة عن بعد كالطابعة أو خادم الملفات. وتتطلب المصادقة من خلال بروتوكول كيربيروس (Kerberos) مشــاركاً إضافيــاً ألا وهو مركز التوزيع الرئيــسي، كما تتطلب أن يكون جميع العناصر الثلاثة التالية أعضاء لنفــس بروتوكول كيربيروس (Kerberos) «الحَيّز» أو (مجال في الدليل النشط):

- العميل الذي يبدأ المصادقة.
- مركز التوزيع الرئيسي (Key Distribution Center) والذي يتكون من عنصرين:
  - خدمة المصادقة.
  - خدمة منح التذاكر.
- الخدمة التي يرغب العميل في الوصول إليها.

وبهذه الإعدادات فإن عملية بروتوكول كيربيروس (Kerberos) موضحة في الشكل (٨-٧). وقبل تمكن العميل من الوصل لبروتوكول كيربيروس (Kerberos) لابد من المصادقة في مركز التوزيع الرئيسي.

(15) http://www.kerberos.org/about/FAQ.html

الشكل (٨-٧): تبادل تذاكر بروتوكول كيربيروس (Kerberos)



أولاً يقــوم كلٌّ من العميل والخدمات بإعلان وجودهما على الشــبكة من خلال تقديم بيانات اعتمادهما ومن خلال طلب «تذكرة - منح - تذكرة» (TGT) (Ticket-Granting-Ticket) (١). وبعــد ذلــك يقوم مركز التوزيع الرئيــسي (KDC) بإصدار تذكرة - منــح - تذكرة (TGT) مشــفرة بمفتاح سري لا يعرفه ســوى مركز التوزيع الرئيسي، كما يقوم بإصدار مفتاح جلسة (session key) يُســتخدم لتشــفير الاستجابات المســتقبلية من مركز التوزيع الرئيسي (٢). والعمر الافتراضي لكل من «تذكرة - منح - تذكرة» (TGT) ومفتاح الجلسة هو ١٠ ساعات يمكن تجديدها من قبل العميل في أي وقت.

وعندما يحتاج العميل إلى خدمة ما فإنه يقوم بطلب «تذكرة خدمة» (Service Ticket) وذلــك لخدمة معينة عن طريق تقديم «تذكــرة - منح - تذكرة» (TGT) إلى مركز التوزيع الرئيسي (KDC) (٣). وإذا تمكن مركز التوزيع الرئيسي (KDC) من فك شــفرة «تذكرة -

منـح - تذكرة» (TGT) فإنه يقـوم بإصدار تذكرة خدمة جديدة لكل من العميل والخدمة المطلوبة (٤). ويقوم العميل بفك شـفرة الجزء الخاص به باسـتخدام مفتاح الجلسة الذي أُرسل في وقت سابق من قِبل مركز التوزيع الرئيسي (KDC)، ومن ثم يقوم العميل بإرسال الجـزء الآخر إلى الخدمـة المطلوبة (٥). وبعد ذلـك تقوم الخدمة بالتحقـق من التذكرة باسـتخدام مفتاح الجلسـة الخاص بها، وهو مفتاح طويل الأجل وصادر من مركز التوزيع الرئيسي (KDC)، وبعد ذلك يُمنح الوصول إلى المستخدم (٦).

ويعـد بروتوكول كيربـيروس (Kerberos) أكثر تقنيات «تسـجيل الدخـول الأحادي» (SSO) شيوعاً في أجهزة الحاسب الآلي المكتبية. ومعظم المنظمات الكبيرة تستخدم أجهزة حاسب آلي مكتبية بنظام ويندوز، كما تستخدم الدليل النشط (Active Directory) لإدارة حسابات المسـتخدمين. وتسـمح المصادقة باسـتخدام بروتوكول كيربيروس (Kerberos) والمتضمـن للدليـل النشـط (Active Directory) للمسـتخدمين بتسـجيل الدخول منذ المرة الأولى لأجهزة الحاسـب الآلي المكتبية، ويسـمح ذلك بالوصـول إلى محركات الأقراص والطابعات البعيدة أو الوصول للتطبيقات البعيدة دون الحاجة لإدخال اسـم المستخدم أو كلمـة المرور. ومـع ذلك فإن بروتوكول كيربيروس (Kerberos) والدليل النشـط (Active Directory) مجهزان لاسـتخدام الشركات، فهما يعملان عندما يصل جميع المستخدمين إلى النظام، وذلك على أجهزة حاسـب آلي موثوقة (تعود ملكيتها وصيانتها عادة للشركة). لكن بروتوكول كيربيروس (Kerberos) ليس مناسـباً للتطبيقات المُستهدفة من قبل مستخدمي الشـبكة الذين يصلـون إلى النظام من خلال أجهزة الحاسـب الآلي الشـخصية. وفي هذه الحـالات فإنه من غير الممكن أن نفترض أن تجار التجزئة والمسـتهلكين لديهم الاسـتعداد للدخول في علاقة ثقة معاً لتبادل تذاكر الخدمة. والتقنيات الموضحة أدناه مصممة للعمل في هذه البيئات الواسعة.

	تسجيل الدخول الأحادي على الشبكة				رابطة اتحادية	
	Kerberos	Token	CAS	SAML	OpenID	OAuth
الإصدار الأول	1987	1995	2001	2003	2005	2006
سياق المصادقة	نظام التشغيل	متصفح الشبكة	متصفح الشبكة	متصفح الشبكة	متصفح الشبكة	التطبيق
ثقة الهوية	عالية جداً	متغيرة حسب التطبيق	عالية	عالية	منخفضة	منخفضة
مقدمو الهوية	أحادي	أحادي	أحادي	متعدد، رابطة اتحادية - قائمة محددة	متعدد، مدخلات المستخدم	متعدد، مدخلات المستخدم
وسيلة التحقق	مفتاح/ مفاتيح سرية	متغير (دالة تجزئة أو مفتاح سري)	توثيق طبقة المنفذ الآمن (SSL certificate)	مفتاح عام	توقيع	توقيع
أمن الرسالة	مشفرة	بدون	بدون	مشفرة وموقعة	موقعة	موقعة
تطبيق العميل/ الخادم	خادم المصادقة، التطبيق، العميل	بدون	خادم المصادقة	خادم المصادقة، التطبيق	التطبيق	التطبيق
التطبيقات	بروتوكول كيربيروس التابع لمعهد ماساتشوستس للتكنولوجيا (MIT)، الدليل النشط	مخصص، فريد لكل عملية نشر	متعدد العملاء ذوي المصدر المفتوح	تطبيقات (Shibboleth) و(Microsoft) و(ADFS)	متعدد العملاء ذوي المصدر المفتوح	متعدد العملاء ذوي المصدر المفتوح
الاستخدام التقليدي	تسجيل الدخول لجهاز الحاسب الآلي، وتطبيقات أجهزة الحاسب المكتبية	تطبيقات الشبكة	تطبيقات الشبكة الداخلية	تطبيقات الشبكة الخارجية مثل (Google Apps) و(Office 365)	تطبيقات الشبكة العامة مثل (Facebook) و(Twitter)	الوصول غير التفاعلي لخدمات الشبكة

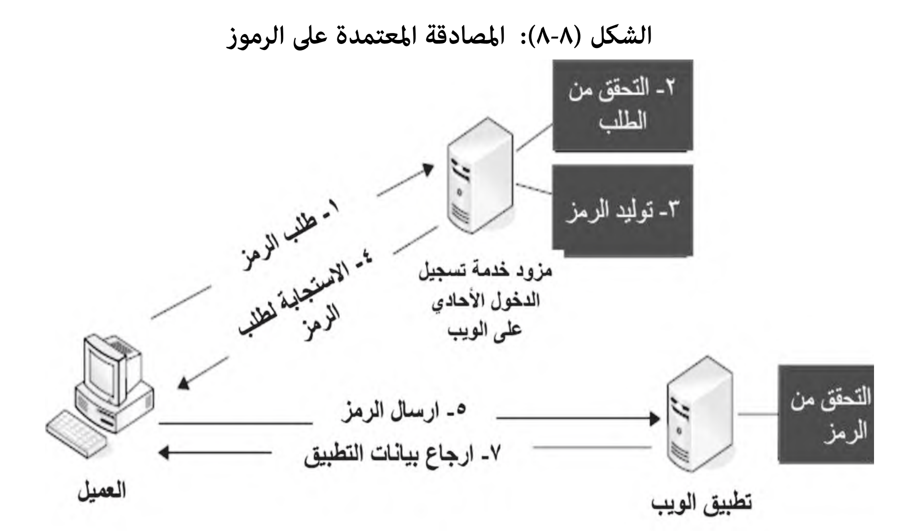
تسجيل الدخول الأحادي على الشبكة (Web single sign-on):

تم تصميــم بروتوكول كيربــيروس (Kerberos) في الثمانينيات وقبــل وقت طويل من إنشــاء شــبكة الإنترنت العالمية (World Wide Web). وعلى الرغم من أن البروتوكول قد تم تحديثه في الســنوات التي تلت ذلك، إلا أنه لم يتم دمجه بســهولة مع تطبيقات شبكة الإنترنت. وهناك سببان لذلك: السبب الأول هو شرط كون جميع العملاء والخوادم أعضاء في نطاق بروتوكول كيربيروس (Kerberos)، وهذا ليس ممكناً مع تطبيقات الشبكة العامة. أما الســبب الآخــر فهو دعم المتصفح - فمتصفحات الشــبكة الرئيســية لا تدعم مصادقة بروتوكــول كيربيروس (Kerberos)، وذلك حتى وقت قريب نســبياً حيــث لا يزال بعضها يتطلب تهيئة واسعة لتمكين الدعم. وتسمح أنظمة تسجيل الدخول الأحادي على الشبكة (Web single sign-on) (WebSSO) للمســتخدمين بالمصادقــة على تطبيق ويب واحد ومن ثم الوصول إلى تطبيقات الشبكة الأخرى دون الحاجة إلى إدخال اسم المستخدم وكلمة المرور مرة أخرى. وهناك العديد من أنظمة تســجيل الدخول الأحادي على الشــبكة حيث نناقش بشكل عام تقنيات المصادقة المستخدمة لتسجيل الدخول الأحادي على الشبكة ومن ثم سنركز على بروتوكول (تسجيل الدخول الأحادي على الشبكة) المستخدم على نطاق واسع في التعليم والشبكات التجارية.

المصادقة المعتمدة على الرموز:

أبســط شكل من أشــكال (تســجيل الدخول الأحادي على الشــبكة) هو استخدام رمز مصادقة مشترك. والمصادقة المعتمدة على الرمز المشترك هي استخدام مُعرِف فريد أو دالة تجزئة مشــفرة تُثبت هوية المستخدم بملكيته للرمز. فعندما يحاول المستخدم للمرة الأولى الوصول إلى أحد تطبيقات الشــبكة المحمية، تتم إعادة توجيه المســتخدم إلى خدمة مزود الرموز للتحقق من اسم المستخدم وكلمة المرور (وأي عوامل مصادقة أخرى مطلوبة)، وبعد ذلك يتم توليد رمز المصادقة (الشكل ٨-٨).

الشكل (٨-٨): المصادقة المعتمدة على الرموز



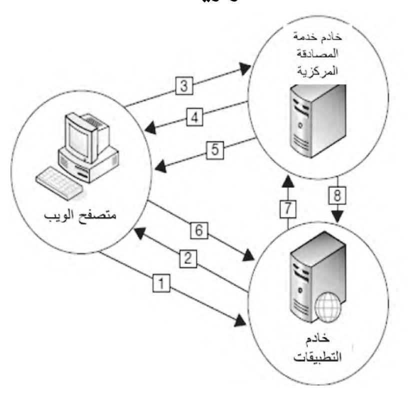
واعتماداً عــلى التنفيذ المحدد لتزويد الرمز فإن رمز المصادقة قد يُســتحدث بعدد من الطرق المختلفة. والأكثر شــيوعاً أن الرمز ينتج من عملية تشفير مثل تمرير اسم المستخدم خلال خوارزمية دالة التجزئة الآمنة (HMAC-MD5) أو خوارزمية تشــفير المفتاح السري (AES). وبمجرد أن يتم توليد الرمز فإنه يتم إعادة توجيه المستخدم إلى الخدمة المطلوبة، كما يتم إضافة الرمز إلى معايير طلب بروتوكول انتقال النص التشــعبي (HTTP). وبديلاً لهــذه العملية يتم حفظ الرمز على شــكل ملــف تعريف الارتبــاط (cookie) في متصفح المســتخدم قبل إعادة توجيه المســتخدم إلى الخدمة المطلوبة. ويتم حفظ ملفات تعريف الارتباط التابعة للجلسة في الذاكرة المؤقتة فقط ويتم حذفها عندما يقوم المستخدم بإغلاق المتصفح. وبالإضافة إلى بيانات المصادقة يُمكن للتطبيقات أن تحفظ بيانات أخرى في ملفات تعريف الارتباط التابعة للجلســة مثل العناصر المحفوظة في عربة التســوق الإلكترونية أو تفضيلات الموقع للمستخدم.

تُعد مشاركة رموز المصادقة في ملفات تعريف الارتباط التابعة للجلسة طريقة سهلة لتفعيل «تسجيل الدخول الأحادي» بين تطبيقات الشبكة المتعددة، لكن القيد الرئيسي لهذه الطريقة هو أن متصفحات الشبكة لا تسمح بمشاركة ملفات تعريف الارتباط بين مجالات متعددة. مثلاً، أحد ملفات تعريف الارتباط التابعة للجلسة المحفوظ في (sunshine.edu) يمكن استخدامه فقط من قبل التطبيقات الموجودة في المجالات الفرعية من (sunshine.edu) مثل مجال (www.sunshine.edu) ومجال (mail.sunshine.edu)، لكن لا يمكن استخدامه في مجال (www.example.com). وإذا كان هناك حاجة لـ «تسجيل الدخول الأحادي» بين تطبيقات في مجالات مختلفة فإنه لا يمكن استخدام ملفات تعريف الارتباط التابعة للجلسة.

وفي تطبيقات الشبكة فإن عملية التحقق من رمز المصادقة تعتمد على الطريقة المتبعة في توليد ذلك الرمز. وفي أبسط الحالات، إذا تم استخدام خوارزمية المفتاح المتماثل فإن تطبيق الشبكة المطلوب سيقوم بإدخال الرمز وإدخال نسخة من المفتاح المشفر إلى خوارزمية فك التشـفير. وتتضمن البيانات الناتجة في الحد الأدنى على اسـم المستخدم للشخص المُصادق، لكنها قد تتضمن بيانات أخرى عن الشخص مثل الاسم، أو بيانات المصادقة الأخرى كالختم الزمني وعنوان بروتوكل الإنترنت (IP).

ويعد «تسجيل الدخول الأحادي» باستخدام المصادقة المعتمدة على الرموز سهل التطبيق نسـبياً، كما يعد آمناً عندما يتم تنفيذه بالشـكل الصحيح باسـتخدام مفتاح تشـفير قوي. لكن هناك بعض المشـكلات. المشـكلة الأولى هي أنه لا يوجد بروتوكول أو نموذج موحد للمصادقة بالرموز، لذلك تقوم كل منظمة بتطبيق نظام المصادقة بشـكل مختلف. وهذه لا تُمثل مشكلة إذا كانت جميع التطبيقات التي ستستخدم «تسجيل الدخول الأحادي» تم تصميمها داخل المنظمة، لكن هذه النقطة تمثل مشـكلة كبيرة عند محاول دمج تطبيقات خارجية. والمشـكلة الأخرى تتمثل في صعوبة التعامل مع إدارة تشفير المفاتيح. فإذا قمت بتوليد مفتاح فريد لكل تطبيق يسـتخدم «تسـجيل الدخول الأحادي» فهناك احتمال أنك تحتاج إلى الإدارة مئات من المفاتيح. ومن جهة أخرى إذا استخدمت مفتاحاً واحداً لجميع الخدمات، وتم اختراق هذا المفتاح، فإن جميع الخدمات ستكون معرضة للخطر.

الشكل (٨-٩): خدمة المصادقة المركزية



بروتوكول خدمة المصادقة المركزية (Central Authentication Service):

يُعد بروتوكول خدمة المصادقة المركزيــة (Central Authentication Service) واحداً من التقنيات الرائدة في «تســجيل الدخول الأحادي» المفتوحــة المصدر، وخصوصاً في مجال التعليــم العالي. وقد تم تطوير هذا البروتوكــول في جامعة ييل (Yale University) في عام ٢٠٠١. ويجمــع بروتوكــول خدمة المصادقــة المركزية بين جوانــب المصادقة المعتمدة على الرموز وبين المفاهيم المستقاة من بروتوكول كيربيروس (Kerberos)، وذلك لجعل «تسجيل الدخول الأحادي» آمناً وســهل التكامل مع معظم تطبيقات الشــبكة (الشــكل ٨-٩). وفي عام ٢٠٠٤ تم نقــل ملكية المشروع إلى منظمــة (Java Architectures Special Interest Group)، وهــي منظمــة تضــم مجموعة من المؤسســات التعليميــة المخصصة لتطوير برمجيات التعليم العالي.

وبشــكل مشابه للمصادقة المُعتمدة على الرموز فإن المســتخدم عندما يحاول الوصول إلى تطبيــق محمي بــ (بروتوكول خدمة المصادقــة المركزية) فإنه يتم إعــادة توجيهه إلى خدمة المصادقة الموجودة على خادم (بروتوكول خدمة المصادقة المركزية). وبشكل مشابه أيضــاً لبروتوكول كيربيروس (Kerberos) فإن هذه الخدمة تقبل بيانات اعتماد المســتخدم وتتحقق منها ومن ثم تقوم بإصدار «تذكرة - منح - تذكرة» (Ticket-Granting-Ticket). وإن أهــم ما يميز (بروتوكول خدمــة المصادقة المركزية) هو أن التذكرة تُحفظ على متصفح

المســتخدم في ملف تعريف الارتباط (cookie) الخاص بالجلســة، وأن خــادم (بروتوكول خدمة المصادقة المركزية) فقط يســتطيع الوصول إلى تلــك التذكرة. وفي الزيارات اللاحقة لخدمة المصادقة في أثناء جلســة تســجيل الدخول لـ (بروتوكول خدمة المصادقة المركزية) (ســاعتان افتراضياً) يعرض المتصفــح «تذكرة – منح - تذكرة» للمصادقــة بدلاً من مطالبة المستخدم بإدخال بيانات الاعتماد الخاصة به.

واســتمراراً لأوجه التشــابه ببروتوكول كيربيروس (Kerberos) فإن المتصفح يطلب من خــادم (بروتوكول خدمة المصادقة المركزيــة) أن يُصدر تذكرة خدمــة (Service Ticket) لتطبيق ويب المحمي. وتذكرة خدمة (بروتوكول خدمة المصادقة المركزية) عبارة عن قيمة عشــوائية يتم اســتخدامها فقط بصفة معرف فريد. ولا يتم حفظ أي بيانات للمســتخدم في تذكرة الخدمة. وتســتخدم تذاكر الخدمة لمرة واحدة فقط حيث يتم التحقق منها مرة واحــدة، وبعد ذلك يتم حذفها مــن خادم (بروتوكول خدمة المصادقــة المركزية). كما أن تذكــرة الخدمة صالحة فقط للموقــع الإلكتروني الذي طُلبَت له التذكــرة، كما أنها صالحة لفترة زمنية قصيرة جداً (الفترة الزمنية الافتراضية هي ١٠ ثوان). وعند توليد تذكرة الخدمة، يتم إعادة توجيه المســتخدم إلى التطبيق الذي طلبه في الأصل بحيث تُضاف تذكرة الخدمة إلى معايير بروتوكول نقل النص التشــعبي (HTTP)، وذلك بشكل مماثل لعملية المصادقة المعتمدة على الرموز.

وبــدلاً من أن يتم التحقق من خلال تطبيق الشــبكة كما يتم في المصادقة بالرموز، فإن تذكرة الخدمة تُرسل مرة أخرى إلى خادم (بروتوكول خدمة المصادقة المركزية) للتحقق. وإذا كان عنوان الموقع الإلكتروني للخدمة يطابق عنوان الموقع الإلكتروني الذي تم طلب التذكرة لــه ولم تنته صلاحية التذكرة، فإن خــادم (بروتوكول خدمة المصادقة المركزية) يســتجيب بوثيقة مكتوبة بـ «لغة الترميز الممتدة» (XML) تحتوي على اسم المستخدم المصادق عليه. وقد أضافت الإصدارات الأحدث من خادم (بروتوكول خدمة المصادقة المركزية) القدرة على استرجاع المواصفات الأخرى كالاسم وعنوان البريد الإلكتروني بالإضافة إلى اسم المستخدم.

وأبرز العوامل الرئيســية وراء نجــاح خادم (بروتوكول خدمــة المصادقة المركزية) هي البســاطة والمرونــة. وعملياً يمكن أن يُضاف دعــم (بروتوكول خدمــة المصادقة المركزية)

بسهولة إلى أي تطبيق ويب إما عن طريق استخدام أحد العملاء المتاحين[16] وإما بتطوير العميل الخاص بك. وخلافاً للمصادقة المعتمدة على الرموز والتي تتطلب خوارزمية تشفير يصعب التعامل معها أحياناً، فإن المتطلب الوحيد للتفاعل مع خادم (بروتوكول خدمة المصادقة المركزية) هو القدرة على إجراء اتصال ببروتوكول نقل النصوص التشعبية المحمي (HTTPS) وتحليل استجابة خادم (بروتوكول خدمة المصادقة المركزية) والتي تكون بـ «لغة الترميز الممتدة» (XML). ويمكن لجميع لغات البرمجة الرئيسية المستخدمة اليوم أن تُلبي هذين المعيارين، لذا فإن تطوير عميل مخصص لـ (بروتوكول خدمة المصادقة المركزية) ليس صعباً. ومن السهل توسيع استخدام خادم (بروتوكول خدمة المصادقة المركزية) لأنه مصمم للمرونة. ويدعم خادم (بروتوكول خدمة المصادقة المركزية) العديد من الأنواع المختلفة لبيانات الاعتماد مثل اسم المستخدم وكلمة المرور في بروتوكول الوصول للدليل Lightweight Directory Access Protocol (LDAP)، وتوثيقات (x.509). كما أنه يمكن ضبط خادم (بروتوكول خدمة المصادقة المركزية) لقبول تذاكر ببروتوكول كيربيروس (Kerberos) مما يؤدي إلى تأسيس حل متكامل لتسجيل الدخول الأحادي - يقوم المستخدم بتسجيل الدخول عند بدء تشغيل جهاز الحاسب الآلي في الصباح دون الحاجة إلى إعادة إدخال كلمة المرور وذلك حتى عند الرغبة في الوصول إلى تطبيقات الشبكة.

الرابطة الاتحادية (Federation):

إن بروتوكول كيربيروس (Kerberos) وبعض من أشكال «تسجيل الدخول الأحادي» توفر جميع الضوابط اللازمة لتأمين التطبيقات داخل المنظمة، لكن ما العمل إذا احتاج المستخدم الوصول إلى تطبيقات خارج المنظمة مثل تطبيقات (Google Apps) و(Office 365)؟ وما الحل في حال احتاج مستخدمون من خارج المنظمة الوصول إلى تطبيقات في منظمتك؟ الإجابة التقليدية لهذا السؤال هي إنشاء حسابات للمستخدمين التابعين لمنظمتك في الأنظمة الخارجية، وإنشاء حسابات «ضيف» في النظام التابع للمنظمة، وذلك لجميع المستخدمين من خارج المنظمة. تخيل أن مجموعة من أعضاء هيئة التدريس في جامعة ولاية الشمس المشرقة يتعاونون مع باحثين من إحدى شركات التكنولوجيا الحيوية المحلية.

(16) https://wiki.jasig.org/display/CASC/Client + Feature+Matrix

والطريقــة الوحيــدة لمنح حق الوصــول إلى البيانات البحثية لــكلا الفريقين تتم بحيث أن جميع موظفي شركة التكنولوجيا الحيوية يحتاجون إلى بيانات اعتماد من الجامعة، وأعضاء هيئة التدريس يحتاجون إلى بيانات اعتماد من شركة التكنولوجيا الحيوية.

وفي نهايــة المطاف فإن هذه العملية غير مدعومة لعدد من الأســباب. الســبب الأول هــو أن هذه العملية تقــدم مجموعة ثانية من بيانات الاعتماد مما يقضي على جميع مزايا «تســجيل الدخول الأحادي». والنقطة الأهم من وجهة نظر أمنية هي أنه لا توجد وسيلة لمعرفة متى يجب ســحب امتيازات المســتخدم الخارجي. فوصول الأفــراد داخل المنظمة يُمكــن أن يُلغى بمجرد أن يتم اكتشــاف أي تغيير في الارتبــاط الوظيفي للفرد (فصل، تغيير في المنصــب الوظيفــي، وغيرها) من قبل نظام إدارة الهوية. لكن هذا النوع من المعلومات عموماً لن يكون متاحاً للأفراد من خارج المنظمة مما يجعل من مراقبة الوصول أمراً صعباً. وبالإضافة إلى الآثار الأمنية فإن إنشاء حسابات في المنظمات الخارجية يتطلب عادة الكشف عن بيانات المســتخدمين الشخصية (مثل الاسم وعنوان البريد الإلكتروني)، مما قد يؤدي إلى مخاوف فادحة تتعلق بالخصوصية.

الرابطة الاتحادية (federation) تسد الفجوة بين أنظمة المُصادقة في المنظمات المختلفة. ويتم تطبيق (الرابطة الاتحادية) من خلال توفير وســيلة للتطبيق الداخلي «مزود الخدمة» (service provider) أو (SP) ليثق في معلومات الفرد (أو «للتأكيد») والمُرســلة من مصدر خارجــي «مزود الهويــة» (identity provider) أو (IdP). في مثال جامعة ولاية الشــمس المشرقة أعلاه، وبدلاً من إنشــاء حسابات لجميع الباحثين في شركة التكنولوجيا الحيوية، فإن النظام الذي يحتوي على البيانات البحثية في الحرم الجامعي لجامعة ولاية الشــمس المشرقة سيقوم بالتحقق من هوية المستخدم عن طريق «مزود الهوية» لشركة التكنولوجيا الحيوية، كما سيقوم النظام بطلب معلومات كافية عن المستخدم لاتخاذ قرار بشأن منح حق الوصول. وإذا نجحت عملية المصادقة وكانت المعلومات الموفرة من قبل «مزود الهوية» (IdP) تُلبي متطلبــات التطبيق، عند ذلك ســيتم منــح الوصول. كما أن طلب المعلومــات واتخاذ قرار بالوصول يتم في كل مرة يقوم فيها المســتخدم بالمصادقة، مما يسمح لجامعة ولاية الشمس المشرقة برفض وصول المســتخدم الذي لم يعد يلبي المعايير، وذلك في أقرب وقت يحصل فيه «مزود الهوية» (IdP) التابع لشركة التكنولوجيا الحيوية على المعلومات.

لكن السماح للمستخدمين التابعين لأكثر من مزود للهوية بالوصول إلى الخدمة يؤدي إلى ظهـور تحد مثير للاهتمام. كيف يمكـن للخدمة معرفة أي من مزودي الهوية (IdP) الذي يسـتطيع مصادقة المسـتخدمين؟ والإجابة تتم من خلال سؤال المستخدمين عن المنظمات التي قاوموا بالاشـتراك فيها. وتقدم خدمة الاكتشاف للمستخدم قائمة بالمنظمات الموثوق بهـا والتي يمكن الاختيار مـن بينها للمصادقة. ويوضح الشـكل (٨-١٠) مثالاً على خدمة الاكتشاف في أحد أنظمة الارتباط الاتحادي الشائعة هو (InCommon).

بروتوكول لغة تمييز التأكيدات الأمنية (Security Assertion Markup Language):

يُعـد بروتوكول لغـة تمييـز التأكيـدات الأمنيـة (Security Assertion Markup Language) (SAML) أحد بروتوكولات الارتباط الاتحادي الأكثر شـيوعاً واستخداماً في برمجيـات المنظـمات. وهو بروتوكـول يعتمد على «لغة الترميـز الممتدة» (XML) تم تطويره في عام ٢٠٠١ مـن قبل لجنة تقنية للخدمات الأمنية تُدعى (OASIS Security Services Technical Committee)[١٧]. وقـد مر هذا البروتوكول بعدد من التنقيحات والإصدارات كان آخرها إصدار (SAML 2.0) والذي أُصدر في عام ٢٠٠٥. ويتضمن هذا البروتوكـول معايير أخرى، بالإضافة إلى معايير «لغة الترميز الممتدة»، وذلك من أجل أمن الرسـائل متضمناً ذلك معايير التشفير والتوقيع. ويُعد أمن الرسائل مهماً في البروتوكول، فلأنـه، بدلاً من إرسـال البيانات مباشرة من «مزود الهويـة» (IdP) إلى «مزود الخدمة» (SP)، يقـوم طرفـا التواصل المعتمدان عـلى بروتوكول «لغة تمييـز التأكيدات الأمنية» بالتواصل من خلال ترحيل الرسائل عبر متصفح المستخدم بلغة ترميز النصوص التشعبية HyperText Markup Language (HTML). وهـذا يُبسـط مـن تهيئـة الارتباطـات الاتحاديـة المعتمدة على بروتوكول «لغة تمييز التأكيـدات الأمنية» (SAML)؛ لأن ضوابط الشـبكة لا تحتـاج إلى تحديث للسـماح لـ «مزود هوية» جديد أو «مـزود خدمة» جديد بالاتصال بالأعضاء الآخرين في الرابطة الاتحادية.

لكن ولأن الرسالة تمر من خلال طرف ثالث غير موثوق به (وهو متصفح المستخدم) فإن رسـائل «لغة الترميز الممتدة» (XML) يجب أن تكون موقعة ومشفرة لضمان أمن الرسالة وتكاملها.

(17) https://www.oasis-open.org/committees/security/

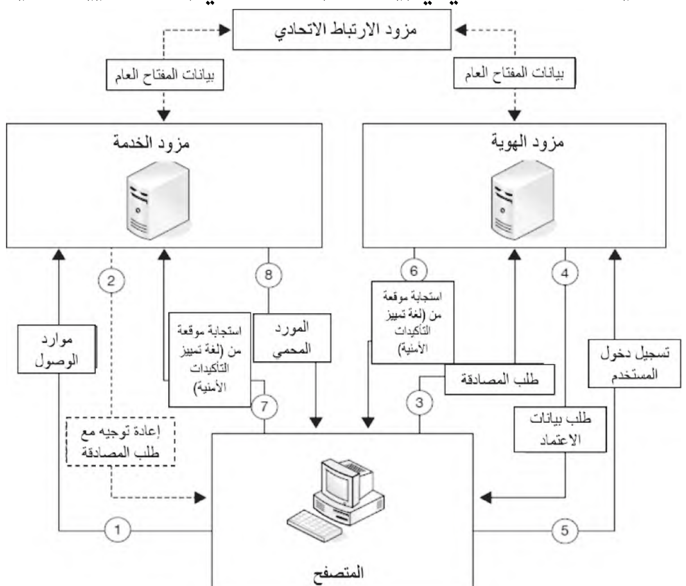
الشكل (٨-١٠): خدمة الاكتشاف في أحد أنظمة الارتباط الاتحادي الشائعة وهو (InCommon)



وفي الارتباطــات الاتحادية الذي تضم عدداً ليس قليلاً من المنظمات ومزودي الخدمات تصبــح المحافظة على تلك الارتباطات معقدة بحيث يمكــن فصلها لتمثل منظمة منفصلة. ويكون مزود الارتباط الاتحادي مســؤولاً عن جميع المهام الإدارية المتعلقة بإدارة شــؤون الاتحــاد، مثل إدارة العضوية، وصياغة سياســات الارتباط وإنفاذهــا، وإدارة البنية التحتية للمفتــاح العــام (Public Key Infrastructure) اللازمــة لعمليات التشــفير. كما يقوم الارتباط الاتحــادي بنشر البيانات الخاصة بالارتباط الاتحادي، وهي عبارة عن مســتندات بـ «لغة الترميز الممتدة» (XML) تحتوي على قائمة شــاملة لأعضاء الارتباط الاتحادي، كما تحتــوي على بيانات هامــة مثل معلومات المنظمة ومعلومــات التواصل، وذلك لكل مزود خدمــة ولكل مزود هوية. ويمثل مزود الارتباط الاتحادي النقطة المركزية في شــبكة الثقة التي تشكل الارتباط الاتحادي. والمشاركون في الارتباط الاتحادي يثقون في أن المزود سيقوم بفحــص الأعضاء الجدد، وذلك للمحافظة على مســتوى معين من الجودة في عمليات إدارة الهويــة. وفي المقابل يقوم المشــاركون بتمويل مــزود الارتباط الاتحادي من خلال رســوم العضوية.

ويوضح الشــكل (٨-١١) عملية مصادقة مُســتخدِم في بيئة الارتبــاط الاتحادي بـ «لغة تمييز التأكيدات الأمنية». فعندما يحاول المستخدم المصادقة من خلال مزود خدمة محمي ببروتوكــول «لغة تمييز التأكيــدات الأمنية» (١)، يقوم مزود الخدمة بالتحقق من أن الموارد المطلوبة تتطلب المصادقة (اختبار الوصول).

الشكل (٨-١١): تسجيل الدخول الأحادي في بيئة الارتباط الاتحادي بـ «لغة تمييز التأكيدات الأمنية»



وإذا كانت المصادقة مطلوبة، فإن مزود الخدمة سيعد نموذجاً بلغة الترميز (HTML) (٢) بحيث يحتوي النموذج على مستند طلب المصادقة بـ «لغة الترميز الممتدة» (XML) والذي سيتم عرضه على خدمة «تسجيل الدخول الأحادي» لدى مزود الهوية (٣). بعد ذلك يقوم مزود الهوية بطلب بيانات اعتماد المستخدم (٤) والتحقق منها (٥). وإذا كانت المصادقة ناجحة فإن مزود الهوية يجمع كافة البيانات عن المستخدم والتي يجب إرسالها إلى مزود الخدمة، كما يقوم مزود الهوية بإصدار رد باستخدام بروتوكول «لغة تمييز التأكيدات الأمنية». ولحماية البيانات الموجودة في هذا الرد فإن مزود الهوية يقوم بتشفير ملف الـ (XML) بالمفتاح العام التابع لمزود الخدمة (والمُسترد من مزود الارتباط الاتحادي)، كما يقوم مزود الهوية بتوقيع المستند بالمفتاح الخاص التابع له. وبعد ذلك يقوم مزود الهوية بإرسال نموذج الـ (HTML) والذي يحتوي على بيانات الرد إلى المستخدم (٦). ويتم تقديم هذا النموذج آلياً إلى مزود الخدمة (٧) الذي يقوم بفك شفرة ملف الـ (XML)، كما يقوم بالتأكد من توقيع الرسالة. الآن وبعد أن تمت مصادقة المستخدم، يقوم مزود الخدمة بتوفير الموارد المطلوبة إلى المستخدم (٨).

وخلافاً لبعض بروتوكولات «تسـجيل الدخول الأحادي» الأخرى والتي تمت مناقشتها في هـذا الفصل، فإن بروتوكول «لغة تمييز التأكيدات الأمنيـة» لم تتم كتابته بصفته جزءاً من تطبيـق الخادم. ويحدد معيار بروتوكـول «لغة تمييز التأكيدات الأمنيـة» تفاصيل كيفية عمل البروتوكول لكن التطبيق الفعلي لهذه التفاصيل ترجع لمطوري التطبيقات. وبسـبب ذلـك أصبح هنـاك العديد من أنظمة المصادقة المختلفة التـي تدعم بروتوكول «لغة تمييز التأكيدات الأمنية» وذلك من أكبر منتجي البرمجيات التجارية مثل أوراكل ومايكروسوفت، وكذلك من التطبيقات المفتوحة المصدر والمتاحة مجاناً.

ويُعد تطبيق بروتوكول «لغة تمييز التأكيدات الأمنية» التابع لشركة مايكروسوفت جزءاً من منتج «خدمات الارتباط الاتحادي للدليل النشـط» (Active Directory Federation Services). ويقدم هذا المنتج خدمة توسـيع نظام الدليل النشـط (Active Directory) لدعـم وصول الارتباط الاتحـادي إلى الموارد المحلية والخارجية باسـتخدام بروتوكول «لغة تمييز التأكيدات الأمنية» والبروتوكولات الأخرى. ويُعد هذا المنتج بمثابة القلب للعديد من منتجات مايكروسـوفت الحديثة، وذلك مع البدء في إصدار المزيد من البرمجيات التي تتبع نموذج الخدمة في اسـتلام البرامج. على سـبيل المثال، إن استخدام هذا المنتج لدعم وصول الارتباط الاتحادي في برامج أوفيس ٣٦٥ (Office 365) يسـمح للمنظمة باستخدام بيانات الاعتماد المحلية (بتسجيل دخول واحد إلى أجهزة الحاسب الآلي المكتبية) للوصول إلى البريد الإلكتروني والتقويم المعتمدين على الحوسـبة السـحابية. ويسـمح توافق هذا المنتج مع معيار بروتوكول «لغة تمييـز التأكيدات الأمنية» للمنظمة بالارتباط الاتحادي مع المنتجات غير التابعة لميكروسوفت مثل (Salesforce.com) و(Google Apps) لقطاع الأعمال.

وتعـد تطبيقات بروتوكول (Shibboleth)، وهي تطبيقـات مفتوحة المصدر ومعتمدة عـلى بروتوكول «لغة تمييز التأكيدات الأمنية»، أكثر التطبيقات شـيوعاً في مصادقة الخادم. وتطبيقـات بروتوكول (Shibboleth) هي تطبيقـات لإدارة الهوية مفتوحة المصدر وذات بنية تحتية للتحكم بوصول الارتباط الاتحادي ومعتمدة على برتوكول «لغة تمييز التأكيدات الأمنيـة» (Security Assertion Markup Language). وتـم تطويـر هذه التطبيقات لتسجيل الدخول الأحادي على الشبكة من قبل (مجموعة إنترنت ٢) (group Internet٢)

والتـــي تتكون مــن مطورين من بعــض الجامعات والمنظــمات البحثيــة. ويحتاج أعضاء هيئــة التدريس والباحثون من مختلف المنظمات إلى طريقة للوصول إلى الموارد المشــتركة والموجودة في الجامعات المختلفة والتي تســتخدم نظام مصادقة فريد يختلف عن الأنظمة الأخرى. وتم إصدار النســخة الأولية من هذه التطبيقات (١,٠) في عام ٢٠٠٣، وتم إحداث تغيــيرات كبيرة في الإصدار الــذي يليه في عام ٢٠٠٥ (إصدار ١,٣) وعام ٢٠٠٨ (إصدار ٢,٠). ومنذ ذلك الحين تم إصدار بعض النسخ التي تحتوي على بعض التعديلات البسيطة. ويعد برتوكول (Shibboleth) الأكثر شيوعاً في المؤسسات التعليمية، وخصوصاً الجامعات البحثية الكبيرة، كما أن هذا النظام هو الأساس في العديد من الاتحادات الوطنية والدولية.

تطبيقات برتوكول (Shibboleth)

يُعرف قاموس ميريام وبستر (Merriam-Webster) مصطلح (Shibboleth) بأنه «العادة أو الاستخدام الذي يُعد بأنه مُميزاً لمجموعة ما عن المجموعات الأخرى»[١٨]. وأتى هذا المصطلح من الكتاب اليهودي المقدس (Hebrew Bible) (6-Judges 12:5) والذي كان يستخدم النطق الصحيح لهذه الكلمة للتمييز بين قبيلة الجلعاديين (Gileadites) (الذين كانوا ينطقون هذه الكلمة بالشكل الصحيح) وقبيلة الإفرايم (Ephraimites) (الذين كانوا ينطقون هذه الكلمة كـ (Sibboleth)).

وفي الوقت نفسه الذي كان يتم فيه تطوير الإصدارات الأولى من بروتوكول (Shibboleth)، كانت القاعدة التي تدير البنية التحتية للشبكات في جميع الجامعات السويسرية، والتي تُدعى (SWITCH)، تتعامل مع القضايا نفسها التي تتعامل معها مجموعة (Internet2) والتي تعمل على بروتوكــول (Shibboleth). وفي عام ٢٠٠٣ أعلنت (SWITCH) عن رابط اتحادي جديد يُدعــى (SWITCHaai)[١٩] والــذي يربط جميع الجامعات بجميــع الشركاء في مجال البحوث والمجال التجاري في ســويسرا مما يســمح للطلاب وأعضاء هيئة التدريــس بالوصول إلى جميع الموارد التعليمية في البلاد عن طريق اســتخدام مجموعة واحدة من بيانات الاعتماد. وبحلول شــهر نوفمبر من عام ٢٠١٢، تضمنت (SWITCHaai) أكثر من ٥٠ مؤسســة تعليمية بوصفها مزودي هوية وما يقارب من ١٠٠ منظمة من القطاع العام والشركات بوصفها مزودي خدمة.

(18) w.merriam-webster.com/dictionary/shibboleth

(19) http://www.switch.ch/aai/about/federation

وبعد النجاح الذي حققته (SWITCH) بتشغيلها رابط اتحادي على نطاق واسع، بدأت الشبكات التعليمية في جميع أنحاء العالم بتطوير خططها للارتباط الاتحادي. ففي عام ٢٠٠٤ أعلنت مجموعة (Internet2) عن ارتباط اتحادي وطني، يُدعى (InCommon)، يربط الجامعات الأمريكية بالشركاء من المؤسسات البحثية الحكومية والشركات. وبدأت (InCommon) بعدد قليل من الأعضاء ونمت في البداية ببطء، لكن مع انضمام شركاء من الشركات الكبرى مثل مايكروسوفت ومع إطلاق بروتوكول (Shibboleth) في عام ٢٠٠٨، تزايد عدد الأعضاء بشكل كبير. وبحلول نهاية عام ٢٠١٢، تضمنت (InCommon) أكثر من ٣٠٠ مؤسسة تعليمية، وهو ما يمثل ما يقارب من ٦ ملايين مستخدم، وأكثر من ١٥٠ من الشركاء من المؤسسات البحثية الحكومية والشركات[٢٠]. وكنظير لـ (SWITCH) و(Internet2) في المملكة المتحدة، أعلنت (JISC) في عام [٢١]٢٠٠٥ عن الارتباط الاتحادي في المملكة المتحدة والتي أصبحت واحدة من أكبر الروابط الاتحادية في العالم متضمنة ما يقارب من ١٠٠٠ مشارك ومئات من مقدمي الخدمات.

بروتوكول (OpenID):

يُعد الارتباط الاتحادي المُعتمِد على بروتوكول «لغة تمييز التأكيدات الأمنية» حلاً ممتازاً لأمن المنظمات، ليكون مصادقةِ الموظفين ومصادقة شركاء العمل، لكنه يتطلب تخطيطاً وتأملاً قبل إضافة أي موارد للارتباط الاتحادي حيث يجب أن يكون كل مزود هوية وكل مزود خدمة مسجلاً في الارتباط الاتحادي قبل استخدامها للمصادقة. ويجب إجراء التسجيل من قبل مسؤولي نظام مزود الهوية، واعتماداً على متطلبات مزود الخدمة، قد يتطلب التسجيل تغييرات في تهيئة النظام التابع لمزود الهوية، وهذا لا يُمثل مشكلة في حال الشركات. فعندما يتم تحديد خدمة ارتباط اتحادي جديدة من قبل الموظفين أو غيرهم من أعضاء المنظمة، فإنه يتم مراجعة المتطلبات والموافقة عليها قبل إجراء أي تغييرات في تهيئة النظام. وهذا يمثل عيباً واضحاً في بروتوكول «لغة تمييز التأكيدات الأمنية» عندما تكون التطبيقات المعتمدة على المستخدم تشمل عامة الناس. تخيل مقدار العمل المطلوب

(20) http://www.incommonfederation.org/participants

(21) http://www.ukfederation.org.uk

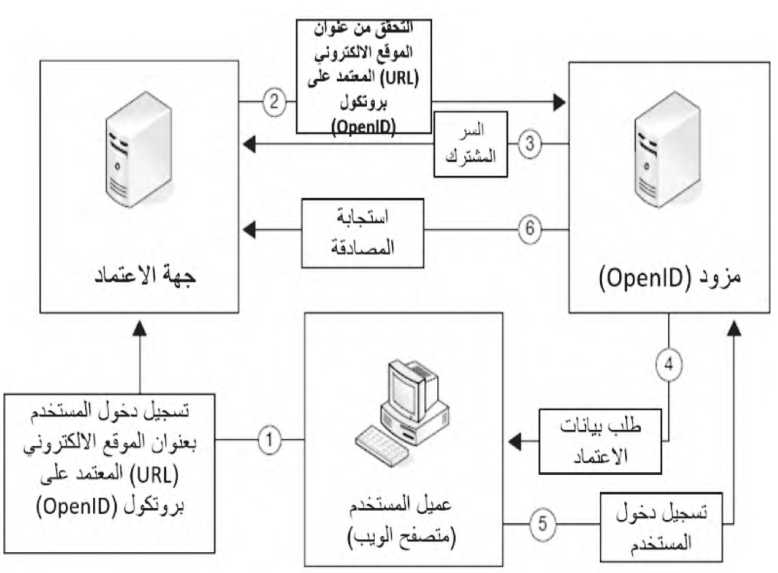
للمحافظــة على الارتباط الاتحادي الذي يحتوي على الملايين من الخدمات ومقدمي الهوية الموجودة على شــبكة الإنترنت مع مئات أو آلاف من مقدمي الخدمات الجديدة التي يتم إنشاؤها يومياً. وللتعامل مع المواقع ذات الكثافة الكبيرة من المستخدمين من جميع أنحاء العالم، مثل تويتر وفيسبوك، يجب استخدام ارتباط اتحادي جديد.

وفي الأصل تم تطوير بروتوكول (OpenID) في عام ٢٠٠٥ لمنصة المدونات (.LiveJournal com). وبدلاً من مطالبة مزود الهوية (والذي يُشار إليه باسم مزود (OpenID)) للتسجيل مــع مزود ارتباط اتحادي مركزي، فإن (OpenID) تســتخدم (النموذج المُوزّع) للمصادقة. والمتطلــب الوحيــد لتصبح مــزود (OpenID) هو وجــود اتصال إنترنت يســمح لأجهزة الحاســب الآلي الأخرى الوصول إليك، ووجــود خادم ويب يعمل على تطبيق خادم متوافق مع (OpenID). وهذه القيود المنخفضة للتعامل مع هذا البروتوكول تعني أن المستخدمين الواعين بشــكل كبير للأمن والخصوصية يمكنهم تشــغيل مزود (OpenID) التابع لهم مما يسمح لهم بتعيين متطلبات القوة وبيانات الاعتماد التي يتم استخدامها لعمليات المصادقة التي يُجريها المستخدمون بأنفسهم. وسبب نجاح هذا البروتوكول هو المنفعة التي يقدمها إلى مــزود الخدمة (وهي جهة الاعتماد في بروتوكول (Relying Party in the) (OpenID (OpenID protocol)). وبدأت بشــائر النجاح لـ «تطبيقات الشبكة» في الظهور مع ظهور بعض المواقع الإلكترونية مثل (Gmail) و(Flickr) و(Facebook) والتي تم إطلاقها جميعاً في عام ٢٠٠٤. ومع ظهور مواقع جديدة تُطلق تطبيقات جديدة في كل وقت، أدى ذلك إلى إحباط المستخدمين بسبب الحاجة إلى التعامل مع حسابات وكلمات مرور متعددة. وأصبح من الســهل نســبياً إضافة دعم بروتوكول (OpenID) وذلك لمطوري التطبيقات ومزودي خدمات البريد الإلكتروني مثل (AOL) و(Google) و(Yahoo) والذين أصبحوا من مزودي (OpenID) في وقت قصير. وبفضل هؤلاء المزودين أصبح بروتوكول (OpenID) يُستخدم في الآلاف مــن المواقع، كما أصبح هناك أكثر من مليار عنوان موقع إلكتروني (URL) تعتمد على بروتوكول (OpenID) قيد الاستخدام على شبكة الإنترنت.

وللمصادقة باســتخدام بروتوكول (OpenID)، يقوم المســتخدم بإرســال عنوان الموقع الإلكــتروني (URL) المعتمــد عــلى بروتوكــول (OpenID) إلى جهة الاعتــماد (Relying

Party) بدلاً من اسم المستخدم (١). ويكون عنوان الموقع الإلكتروني (URL) المعتمد على بروتوكول (OpenID) فريداً لكل مســتخدم، ويكون عادة مجــالاً فرعياً للمنظمة المزودة لـــ (OpenID)، عــلى ســبيل المثــال (http:// jsmith.sunshine.edu). ثم تطلب جهة الاعتــماد عنوان الموقع الإلكــتروني (URL) ويتم إعادة توجيهها إلى مزود (OpenID) (٢). ويستجيب مزود (OpenID) بسر مشترك بحيث يُستخدم هذا السر في مصادقة الاستجابة (٣). وبعد ذلك تقوم جهة الاعتماد بإعادة توجيه متصفح المستخدم إلى مزود (OpenID) وذلك للمصادقة. وبمجرد أن يقوم المســتخدم بتزويد بيانات اعتماده (٤) ويقوم بروتوكول (OpenID) بالتحقــق من صلاحيــة بيانات الاعتماد تلــك (٥)، يقوم البروتوكول بإنشــاء استجابة للمصادقة ويقوم بإرجاعها مع السر المشترك إلى جهة الاعتماد (٦). وبمجرد مصادقة المســتخدم يتم ربط عنوان الموقع الإلكــتروني (URL) المعتمد على بروتوكول (OpenID) بحســاب محلي في تطبيق جهة الاعتماد، كما يتم طلب بيانات المســتخدم اللازمة للخدمة (الاسم، وعنوان البريد الإلكتروني، وغيرها). وهذه العملية موضحة في الشكل (٨-١٢).

الشكل (٨-١٢): بروتوكول (OpenID)



وتـــم إطلاق المواصفـــات النهائيـــة لبروتوكـــول (OpenID 2.0)[٢٢] في أواخر عام ٢٠٠٧ متضمنة القدرة على إطلاق سمات المستخدم بالإضافة إلى استجابة المصادقة أو ما يُدعى بـ «تبادل الســـمات في بروتوكول (OpenID Attribute Exchange)» (OpenID)[٢٣]. كما يضيف بروتوكول (OpenID 2.0) دعماً للهويات الموجهة التي تســـمح للمستخدم بإدخال اســـم المجال لمزود (OpenID) (على ســـبيل المثال « yahoo.com») أو اختيار المزود من قائمة، وســـتقوم قائمة اكتشـــاف مركزية لدى المزود بإرجاع عنوان الموقع الإلكتروني (URL) الصحيح والمعتمد على بروتوكول (OpenID) إلى المستخدم.

ويوضح الشـــكل (٨-١٣) شاشـــة اختيار لمزود تقليدي باســـتخدام جهة اعتماد بروتوكول (OpenID 2.0). ويُعد إطلاق المواصفات ميزة هامة لأنه يسمح للمستخدمين بتجاوز نماذج طلب (معلومات المســـتخدم الأساسية) مثل الاســـم وعنوان البريد الإلكتروني من خلال تأكيد مزود (OpenID) التابع لهم لتلك المعلومات. ولأن عملية التسجيل وعملية تسجيل الدخول أصبحت أســـهل للمســـتخدم، لاحظت جهات الاعتماد زيادة ملحوظة في التسجيل واستخدام الخدمة عند استخدام مصادقة بروتوكول (OpenID)[٢٤]. ويمكن النظر أيضاً إلى نظام إطلاق المواصفات في بروتوكول (OpenID 2.0) باعتباره مكسباً لخصوصية المستخدم. فقبل إطلاق أي بيانات إلى جهة الاعتماد، يسعى مزود (OpenID) للحصول على إذن المستخدم، ويسمح للمستخدم بإنهاء المعاملة إذا كان لا يرغب في الإفصاح عن البيانات المطلوبة.

الشكل (٨-١٣): شاشة اختيار لمزود بروتوكول (OpenID 2.0)



المصدر: Janrain

---

(22) http://openid.net/specs/openid-authentication-2_0.html

(23) http://openid.net/specs/openid-attribute-exchange-1_0.html

(24) http://janrain.com/resources/industry-research/consumer-perceptions-of-online-registration-and-social-login

بروتوكول (OAuth):

تـم تصميم بروتوكـول (OpenID) للتعامل مع حالة الاسـتخدام التقليدية لتطبيقات الشـبكة - والمتمثلة في شـخص ما يجلس أمام متصفح الشـبكة للوصول إلى الخدمة. لكن وبعـد تطوير بروتوكـول (OpenID) بوقت قصـير ظهرت حالتان جديدتـان من حالات الاسـتخدام وهما: مواقع وتطبيقات الشـبكة التي تعتمد على المزج بين محتويات الشبكة الأخرى (web mashups)، وتطبيقات الأجهزة المحمولة. الاسـتخدام الأول وهو الـ (web mashups)، وهـو عبارة عن صفحة ويب أو تطبيق تقـدم خدمة جديدة من خلال دمج بيانات واحد أو أكثر من واجهة برمجة التطبيقات (API) على الإنترنت. على سبيل المثال، الموقع الإلكتروني لمنظمة (BigHugeLabs) (http://bighugelabs.com) يسـتخدم صور واجهـة برمجة التطبيقات من موقع (Flickr) لإنشـاء الملصقات، والصـور المزينة، وأنواع أخرى عديدة من الصورة الجديدة. ويوجد الآلاف من المواقع التي تستخدم واجهة برمجة تطبيقات خرائط جوجل (https://developers.google.com/maps) (Google Maps) ويمكن من خلال هـذه التطبيقات أخذ جولة عـلى مصانع الخمور في أي مكان في الولايات المتحدة (http://winesandtimes.com) كما يمكن رؤية التوجهات الحالية لموقع تويتر حسب الموقع (http://trendsmap.com) (الشكل ٨-١٤). ولا يمكن حماية واجهة برمجة التطبيقات المستخدمة من قبل الـ (mashups) بواسـطة بروتوكول (OpenID) لأنه لا يتم الوصول إليها بواسـطة شخص يسـتطيع المصادقة على مزود (OpenID)، بل يتم الوصـول إلى واجهة برمجة التطبيقات بواسطة تطبيق ويب يمزج البيانات ويُنشئ الـ (mashups).

الشكل (٨-١٤): (http://trendsmap.com)



وبالمثــل فإن تطبيقات الأجهــزة المحمولة مثل الهواتف الذكيــة والأجهزة اللوحية تقوم بالوصــول إلى واجهــة برمجة التطبيقات على شــبكة الإنترنت لاســترجاع ومعالجة البيانات للمســتخدم لتعزيز قدراتهــم المحلية. مثلاً في حال حصولك على نقــاط عالية في لعبة على الهاتف الذكي فإن هذه اللعبة قد تســمح لك بتحديث حالتك على تويتر أو فيسبوك، ولكنك لــن ترغب في منح حق الوصــول الكامل (لتحديث قائمة الأصدقاء الخاصة بك، على ســبيل المثــال) لمطــور اللعبة. لذلك هناك حاجة لبروتوكول يســمح للمســتخدم بمنح التطبيق أو الخدمــة حق الوصول لموارد محددة ولفترة محدودة من الوقت دون إعطاء بيانات الاعتماد الخاصــة به. وقد تم تطوير بروتوكــول (OAuth) أو بروتوكول «التصريح المفتوح» (open authorization) لتلبيــة هذه الحاجة. ووفقاً للصفحة الرئيســية لتقنية (OAuth)[٢٥] فإن هذا البروتوكول هو آلية تســمح للمســتخدم منح حق الوصول من موارد خاصة في موقع ما (مزود الخدمة) إلى موقع آخر (العميل). ويوضح الشكل (٨-١٥) لمحة عامة عن البروتوكول.

وأول شيء يجــب عليــك أن تعرفه عن بروتوكــول (OAuth) هو أنه ليــس بروتوكولاً للمصادقــة عــلى الرغم من أن الكثير مــن الناس يعتقد بالخطأ أنه كذلــك. وفي الواقع أن بروتوكول (OAuth) يتعامل مع المصادقة حيث يعمل على توفير تطبيق الشــبكة (عميل-OAuth) بوسيلة لطلب الوصول إلى واحد من الموارد أو أكثر (النطاق) من المستخدم (مالك الموارد) من خلال خادم التصريح التابع لبروتوكول (OAuth)، ويكون قادراً على اســتخدام التصريح لفترة زمنية ممتدة، كما يسمح للمستخدم بإلغاء الوصول في أي وقت.

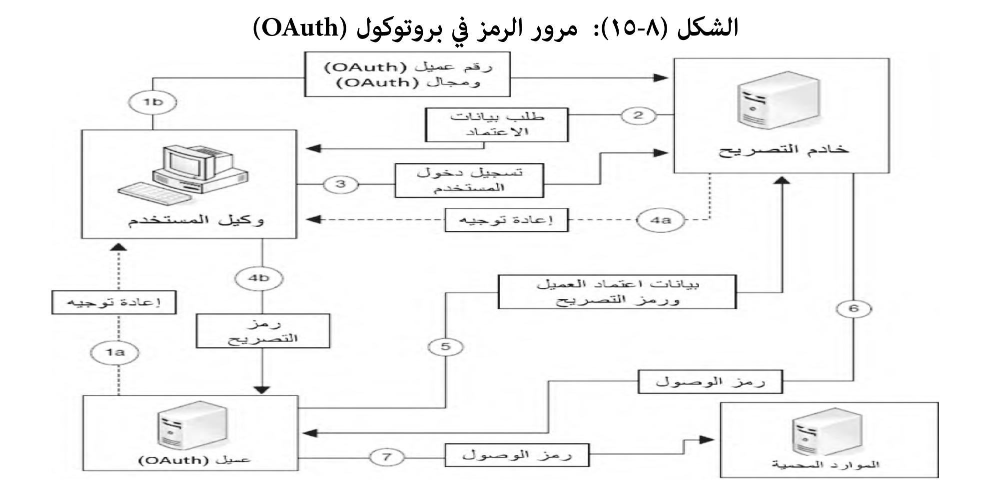
وقبل أن يتمكن العميل من إرسال الطلبات إلى خادم التصريح، يجب أن يقوم التطبيق بتسجيل أحد المُعرّفات مع الخادم، كما يجب أن يتلقى بيانات اعتماد العميل، والتي تكون عادة في شــكل كلمة مرور أو سر مشــترك. فعندما يحتاج العميل إلى الوصول إلى مورد ما لأول مرة يتم إعادة توجيه وكيل المستخدم التابع لمالك الموارد (المتصفح أو تطبيق الأجهزة المحمولــة) إلى خادم التصريح مع نطاق الطلب ومعرف العميل (1a & 1b). ويقوم خادم التصريح بمصادقة المستخدم (٢ & ٣) (قد يطلب بيانات الاعتماد مباشرة، أو على الأرجح أن تكون جزءاً من الارتباط الاتحادي/ شبكة تسجيل الدخول الأحادي) ويقدم قائمة من الموارد المطلوبة ويمنحهم فرصة لقبول أو رفض الطلب.

(25) http://oauth.net/about/

وإذا قـام مالك المـورد منح حق الوصول فإنــه يتم إعادة توجيه وكيل المســتخدم إلى عميل بروتوكول (OAuth) مع رمز التصريح (4a & 4b). بعد ذلك يقوم عميل (OAuth) بإرســال رمز التصريح وبيانات اعتماد العميل والتي أنشــئت سابقاً مع خادم التصريح (٥). ويقــوم خادم التصريح بالتحقق من بيانات اعتماد العميــل وطلبه ثم يُصدر رمزاً للوصول (٦) والذي يســتطيع العميل اســتخدامه للوصول للموارد المحمية (٧). ويســتطيع عميل (OAuth) الاستمرار في استخدام رمز الوصول حتى نهاية مدته الزمنية أو حتى يقوم مالك الموارد بتعطيله.

وتعمل معظم مواقع شــبكات التواصل الاجتماعي بما في ذلك الفيسبوك (Facebook) وتويتر (Twitter) وفورسكوير (Foursquare) وجوجل بلس (+Google) على توفير الوصول إلى خادم التصريح في بروتوكول (OAuth). وإذا كنت في أي وقت مضى قد سمحت لتطبيق ما أن يعلق على جدولك الزمني في فيسبوك، أو أن يضع رسالة في حساب تويتر الخاص بك، فعندها تصبح أنت مالك الموارد في معاملة (OAuth). والمشــكلة الرئيســية في بروتوكول (OAuth) أن مصادقة المستخدم متروكة إلى خادم التصريح مما يعني أن المستخدم إذا كان لديــه عملاء يرغبــون في الوصول إلى ثلاث خدمات مختلفة تســتخدم مصادقة (OAuth)، عندهــا يتوجــب عليهم المصادقة ثلاث مــرات منفصلة. ويعتقد الكثــير من المطورين أن بروتوكول (OAuth) «جيد بما فيه الكفاية» كنظام مصادقة، وذلك لأن المطورين يشــعرون بأنــه إذا كان خادم التصريــح يُصدر رمز التصريح لطلب بروتوكــول (OpenID) فإنه يتم التحقق من هوية المستخدم كما يتم الثقة في المصادقة.

الشكل (٨-١٥): مرور الرمز في بروتوكول (OAuth)



وإذا استُخدم رمز وصول بروتوكول (OAuth) للمصادقة والتصريح فإن هناك إمكانية أن يقوم العميل السـيئ بإسـاءة استخدام الرمز وانتحال شـخصية المستخدم في أي موقع آخر يسـتخدم خدمة التصريح نفسها. وفي مُعظم التطبيقات التي يُستخدم فيها بروتوكول (OAuth)، فـإن مخاطر هذا النـوع من الهجمات تُعد الأقل لأن الموارد المحمية ببروتوكول (OAuth) (شـبكات وسـائل التواصل الاجتماعي، والمدونات الإلكترونيـة، وغيرها) لا تُعد موارد ثمينة. ومع بدء المصارف البنكية والمؤسسـات الماليـة تطبيق بروتوكول (OAuth) أصبـح الهدف أكـثر قيمة وأكثر عرضة للاسـتغلال. ويوجد بروتوكول مُقـترح حديثاً وهو بروتوكـول (OpenID Connect) والـذي يجمـع بـين بروتوكـول (OAuth) للتصريح، وبروتوكـول (OpenID) للمصادقة، كما يضم عناصر مـن بروتوكول «لغة تمييز التأكيدات الأمنية» وذلك لأمن الرسـائل في معيار واحد[٢٦]. ومـا زال هناك الكثير لإضافته في تصميم بروتوكـول (OpenID Connect)، ومـا زال أمـام هذا البروتوكول العديد من السـنوات للوصول إلى شـعبية بروتوكول (OAuth)، لكن هذا البروتوكول جدير بالذكر كتقنية لاحقة لبرتوكول (OAuth).

وهناك طريقة مبسـطة لمعرفة كيفية اسـتخدام بروتوكول (OAuth) في الواقع العملي من خلال إنشاء تطبيق (MVC 4) باستخدام قالب من قوالب الإنترنت في برنامج (Visual Studio ٢٠١٢). ويقـدم تطبيق (MVC 4) آلية تتضمن بروتوكول (OAuth) بوصفه أحد مواصفاتها لمصادقة المسـتخدم وتسمى هذه الألية بـ (SimpleMembershipProvider). ولتنفيذ بروتوكول (OAuth) يقوم تطبيق (MVC 4) باستخدام جدول يسمى (webpages_OAuthMembership)، والموضحة هيكلته في الشكل (٨-١٦). ويعد عمود (Userid) هو المفتاح الأسـاسي لسـجل المسـتخدم في التطبيق المحلي. ومن خلال جدول (webpages_OAuthMembership)، وتقـوم آليـة (SimpleMembershipProvider) بربط مُعرِف المسـتخدم المحلي بالمعلومات التعريفية للمسـتخدم والموجودة لدى المـزود البعيد مثل فيسـبوك وتويتر. وبمجرد تكوين هذا الربط يسـتطيع المستخدم عندها من تقديم بيانات اعتماده للمزود البعيد. ويقوم التطبيق المحلي بالتحقق من تلك البيانات مع المزود البعيد، وإذا أكدها الطرف الثالث، يتم السماح للمستخدم بالوصول إلى التطبيق المحلي.

(26) http://openid.net/connect

وتجدر الإشـارة إلى أن المسـتخدم، وليس التطبيـق، هو من يقوم بالربـط بين مُعرِف المسـتخدم المحـلي والمُعرِف لـدى الطرف الثالث، وعـلى ذلك فإن التطبيق يسـمح فقط للمستخدم بإنشاء تلك الرابطة.

الشكل (٨-١٦): تطبيق (UserId) و(ProviderUserId)

dbo.webpages_OAu...embership [Data] | dbo.webpages_OAu...mbership [Design]

Max Rows: 1000

	Provider	ProviderUserId	UserId
*	NULL	NULL	NULL

نموذج حالة-ماركوس هِس (Markus Hess):

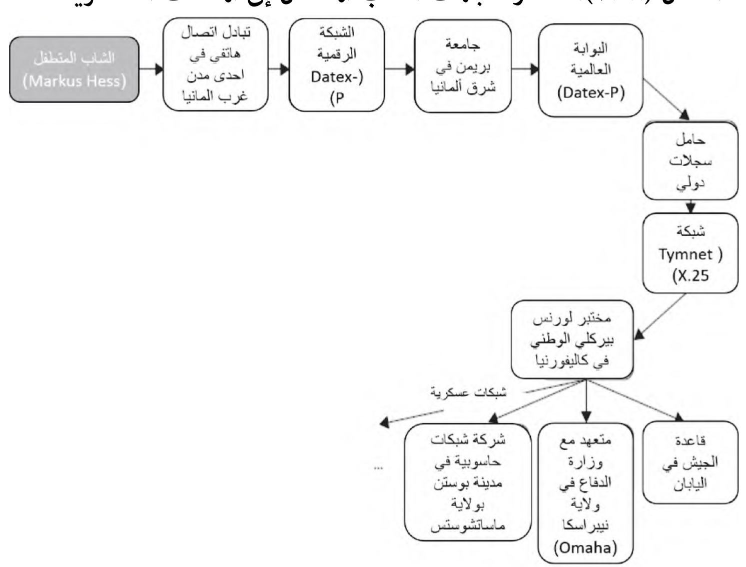
اسـتخدم كليف سـتول (Cliff Stoll)، وهو عالم فضاء وهـاوي لتقنية المعلومات، قوة الملاحظة الحادة لديه لتعقب شـاب ألماني متطفـل يُدعى ماركوس هس (Markus Hess) والذي تمكن من الدخول بنجاح للعديد من المنشـآت العسـكرية الأمريكية على مدى عام خلال الفترة ١٩٨٦-١٩٨٧. وبعد حصول هذا الشاب المتطفل على العديد من الملفات، قام ببيعها لمخابرات الاتحاد السـوفيتي السابق (KGB). وبغض النظر عن إصرار هذا الشاب المتطفـل ومهارتـه فقد تمكن من الدخول إلى أجهزة الحاسـب الآلي في معظم الحالات من خلال استغلال كلمات المرور الضعيفة. ويوضح الشكل (٨-١٧) مسار هجمات هذا الشاب المتطفل إلى المنشآت العسكرية.

وبمراقبة المطبوعات التفصيلية لنشاط الشاب المتطفل اتضح أنه حاول دخول قرابة ٤٥٠ جهاز حاسـب آلي، وذلك باستخدام أسماء الحسابات الشائعة مثل (roof)، أو (guest)، أو (system)، أو (field) بالإضافة إلى كلمات المرور الافتراضية أو الشـائعة. وباستخدام بعض الأدوات البرمجية البسيطة مثل (who) و (finger)، والتي تدون بيانات المستخدمين الذين تم تسـجيل دخولهم إلى النظام، استطاع الشـاب المتطفل من إيجاد أسماء حسابات فعلية لبعض المستخدمين. وفي نحو (٥٪) من الأجهزة التي حاول الشاب المتطفل اختراقها، كانت أسـماء الحسـابات الافتراضية وكلمات السر صحيحة، على الرغم من أنـه كان من المتوقع أن تكـون تلـك الأجهزة آمنة. وغالباً مـا تعطي بيانات الاعتـماد الافتراضية تلك امتيازات

مدير النظام أيضاً. وفي بعض الحالات كان يحاول الشـــاب المتطفل بمجرد دخوله إلى النظام اســـتغلال نقاط ضعف البرمجيات المعروفة لرفع مســـتوى الامتيازات ليصبح مديراً للنظام. وفي حالات أخرى كان يستغل المشكلات التي حظيت بتغطية إعلامية في العديد من أنظمة التشغيل للحصول على «الجذر» ولتحقيق امتيازات مدير النظام.

وقام هذا الشـــاب المتطفل أيضاً بكسر كلمات المرور المشفرة، حيث كان نظام التشغيل المستخدم هو نظام ينكس (UNIX) والذي يحفظ كلمات المرور بصيغة مشفرة لكنه يضعها في مكان مقروء علناً. وأظهرت سجلات حركة المرور في النظام أن الشاب المتطفل كان يقوم بتحميل ملفات كلمات المرور المشفرة من الأنظمة المُخترقة إلى جهازه الشخصي، وبعد قرابة أســـبوع يقوم بإعادة الاتصال بنفس أجهزة الحاسب الآلي المُخترقة ويقوم بتسجيل الدخول إلى حســـابات قائمة وبكلمات مرور صحيحة. وبعـــد التحقيق اتضح أن كلمات المرور التي تم تخمينها بنجاح كانت كلمات إنجليزية - أســـماء شـــائعة، أو أسماء أماكن، مما يشير إلى اســـتخدام هجمات القاموس حيث قام بتشفير كلمات القاموس بالتسلسل ومقارنة النتائج بكلمات المرور التي قام بتحميلها سابقاً.

الشكل (٨-١٧): مسار هجمات الشاب المتطفل إلى المنشآت العسكرية



وســاعدت هــذه التجربة المحققين على إدراك الضعف في أمــان كلمات المرور في بعض الإصــدارات من نظام ينكس (UNIX)، كما ســاعدت على إدراك آثــار ذلك الضعف. وفي ذلــك الوقت كانت إصدارات نظام ينكس (UNIX) تفتقــر إلى اعتبار بعض كلمات المرور متقادمــة ومنتهيــة الصلاحية، كما تفتقر إلى اســتثناء كلمات القامــوس من كلمات المرور. وأيضاً لا يُعد الســماح لأي شخص بقراءة كلمات المرور والثقة في أمن نظام التشفير مناسباً في تلك الإصدارات من نظام ينكس. ولم تهتم المبادئ التوجيهية الصادرة من مختبر لورنس بيركلي الوطني (Lawrence Berkeley lab) بتعزيز اختيار كلمات مرور جيدة مما أدى إلى إمكانية تخمين (٢٠٪) من كلمات مرور المستخدمين باستخدام كلمات القاموس.

المراجع:

Stoll. C. «Stalking the wily hacker,» Communications of the ACM, May 1988,31(5): 484-497

Stoll. C. «The Cuckoo's egg,» Doubleday, http://en.wikipedia.orgl wikilThe_ Cuckoo 's_Egg

الملخص:

في هذا الفصل استعرضنا عمليات إدارة الهوية وإدارة الوصول بدءاً من هوية المستخدم في نظام الســجلات ووصولاً لآليات المصادقة والتصريح. كما استعرضنا مراحل إدارة الهوية - اكتشــاف الهوية، وملاءمة الهوية، وإثراء الهوية. كما اســتعرضنا كيفية استخدام (سياسات التحكم في الوصول المعتمد على الدور) في إدارة الوصول.

والمصادقة هي العملية المُســتخدمة في التحقق من هوية صاحب الحســاب. وتتطلب المصادقة نوعين من المعلومات: الأول أســاسي (اســم المســتخدم) والثاني بيانات الاعتماد. وبيانــات الاعتماد يمكن تقســيمها إلى ثلاث فئــات عريضة هي: كلمات المــرور، والقطع الرمزية، والقياسات الحيوية. والمصادقة المتعددة العوامل تتطلب اثنين أو أكثر من بيانات الاعتماد المختلفة حتى تُستخدم معاً للتحقق من صحة الهوية.

وتســمح أنظمة «تســجيل الدخول الأحادي» للمســتخدمين بالوصــول إلى التطبيقات الموجودة في الأنظمة المتعددة داخل المنظمة الواحدة عن طريق المصادقة لمرة واحدة فقط.

وبعض بروتوكولات «تسـجيل الدخول الأحادي»، مثـل بروتوكول كيربيروس (Kerberos)، مصمم للاسـتخدام على الأجهزة الحاسـوبية المكتبية. وبعضها الآخر، مثل برتوكول (خدمة المصادقـة المركزيـة) وبروتوكول المصادقـة المعتمدة على الرموز، مصمم للاسـتخدام على تطبيقات الشـبكة. أمـا برتوكـولات الارتباط الاتحادي مثـل بروتوكـول (Shibboleth) وبروتوكول (OpenID) فإنها تسـمح للمسـتخدمين من منظمات متعـددة بالوصول إلى الموارد المشتركة، وتقوم بتوسيع تجربة «تسجيل الدخول الأحادي» خارج المنظمة الواحدة.

أسئلة مراجعة للفصل:

١. ما إدارة الهوية؟

٢. اشرح باختصار نموذج مراحل إدارة الهوية.

٣. ما نظام السجلات (Systems of Records)؟

٤. هل يُعد اسم الشخص مُعرِفاً جيداً في نظام السجلات؟ علل إجابتك.

٥. ما الدور الذي يلعبه سجل الشخص (Person Registry) في عملية إدارة الهوية؟

٦. ما الدور؟

٧. ما فصل المهام؟

٨. أعط مثالاً على سياسات التحكم في الوصول المعتمدة على الدور؟

٩. ما الذي تقوم به عملية تدقيق الوصول؟

١٠. ما بيانات الاعتماد؟

١١. ما التصنيفات الثلاثة لبيانات الاعتماد؟

١٢. ما أقدم شكل من أشكال بيانات الاعتماد وأبسطها؟

١٣. ما الفرق بين هجمات القاموس وهجمات القوة الغاشمة؟

١٤. اذكر ميزة واحدة وعيباً واحداً لكل نوع من أنواع بيانات الاعتماد التالية:

- كلمات المرور.
- البطاقات الذكية.
- القطع الرمزية.
- مقارنة القياسات الحيوية.

١٥. ما العوامل السبعة التي يجب أخذها في الاعتبار عند تحديد مدى ملاءمة العلامات الحيوية؟

١٦. اذكر ثلاثة من إيجابيات «تسـجيل الدخول الأحادي» وثلاثة من سلبياتها واشرحها باختصار.

١٧. ما اسم هيكل «تسجيل الدخول الأحادي» التابع لشركة مايكروسوفت؟

١٨. ما رمز المصادقة؟

١٩. اذكر ميزة واحدة وعيباً واحداً لما يلي:

- الرمز المشترك.
- بروتوكول (خدمة المصادقة المركزية).
- بروتوكول (Shibboleth).
- بروتوكول (OpenlD).
- بروتوكول (OAuth).

٢٠. اذكـر وجهاً واحداً من أوجه التشـابه بـين بروتوكول (خدمـة المصادقة المركزية) وبروتوكول (Kerberos).

٢١. ما الغرض من الارتباط الاتحادي؟

٢٢. أين تم تأسيس أول ارتباط اتحادي بواسطة بروتوكول «لغة تمييز التأكيدات الأمنية» (Security Assertion Markup Language)؟ وماذا كان يُسمى؟

٢٣. اذكر الأدوار الأربعة للارتباط الاتحادي بواسطة بروتوكول «لغة تمييز التأكيدات الأمنية» واشرح كلاً منها.

٢٤. اشرح اثنين من الاختلافات في الخصائص بين بروتوكول (OpenID 2.0) وبروتوكول (OpenID 1.0).

٢٥. ما المواقع والتطبيقات التي تعتمد على المزج بين محتويات الشبكة الأخرى (web mashups)؟ ولماذا تعتمد في وظائفها على بروتوكول (OAuth)؟

أسئلة على نموذج الحالة:

١. ما هي بعض الأنشطة التي تقوم بها حالياً مختبرات لورنس بيركلي الوطني (Lawrence Berkeley lab)؟

٢. في رأيك ما المعلومات القيمة التي قد يتمكن المهاجم من الحصول عليها في حال الدخول غير المصرح به لأجهزة الحاسب الآلي في تلك المختبرات؟

٣. ما الخطوات التي تم اتخاذها في تلك المختبرات للحد من احتمال الوقوع في تلك الاختراقات؟ (يجب أن تكون قادراً على إيجاد هذه المعلومات من الإنترنت).

٤. ما نظام التشغيل الذي تستخدمه في أكثر الأحيان؟

٥. كيف تستطيع مراقبة جميع الحسابات وخصائصها في نظام التشغيل هذا؟

٦. هل يوجد حسابات افتراضية للمستخدم في نظامك (ضيف، مسؤول النظام، وغيرها)؟

٧. إذا كان نظامك يحتوي على تلك الحسابات، هل ترى أي ثغرات محتملة في جهاز حاسبك الآلي بسبب هذه الحسابات؟

٨. إذا كانت إجابتك (نعم) للسؤال السابق، ما الذي يمكنك القيام به لإصلاح تلك الثغرات؟

نشاط التدريب العملي - تطابق الهوية والدمج:

هذا النشاط يوضح عملية تطابق الهوية والدمج المستخدمة من قبل سجل الشخص أثناء مرحلة ملاءمة الهوية في عملية إدارة الهوية. وستقوم بمقارنة نظامين مختلفين للسجلات في جامعة ولاية الشمس المشرقة وستقوم بإنشاء ملف واحد للبيانات.

١. قم بتحميل جدول (human_resources.xls) والذي يحتوي على بيانات هوية الموظف من نظام الموارد البشرية وذلك من الموقع الإلكتروني المصاحب للكتاب.

٢. قم بتحميل جدول (studencsystem.xls) والذي يحتوي على بيانات هوية الطالب من الموقع الإلكتروني المصاحب للكتاب.

٣. قم بتحميل جدول سجل الشخص (person_registry.xls) من الموقع الإلكتروني المصاحب للكتاب.

٤. باستخدام مخطط تدفق البيانات في الشكل (٨-٢) قم بعملية المطابقة والدمج للبيانات في جدول الموارد البشرية وجدول الطالب.

٥. قم بتسجيل نتائج عملية المطابقة والدمج في جدول سجل الشخص.

النتائج المطلوب تسليمها: قم بتسليم محتويات جدول سجل الشخص إلى أستاذ المادة.

مثال:

بيانات الموارد البشرية:

الدور	المسمى الوظيفي	الإدارة	الكلية	تاريخ الميلاد	اسم العائلة	الاسم الأول	الرقم التعريفي
إداري	مساعد أستاذ	الهندسة الكهربائية	الهندسة	٠٧/٠٥/٩٢	ميرز	سوزان	١٠٠٣٤٥٥
عضو هيئة تدريس	بروفسور	الكيمياء	كلية العلوم	٠١/٢٣/٨٨	سمث	جون	١٠٠٣٤٥٦

بيانات الطالب:

الإدارة	الكلية	تاريخ الميلاد	اسم العائلة	الاسم الأول	الرقم التعريفي
علوم الحاسب	الهندسة	٠٧/٠٥/٩٢	ميرز	سوزان	U٨١٢٣٦٥٨
تاريخ	الأداب	٠٩/١٢/٩٠	جونسون	ديفد	U٧٦٣٤١٠٦

نتائج بيانات سجل الشخص:

الدور الأساسي	الرقم الوظيفي	رقم الطالب	تاريخ الميلاد	اسم العائلة	الاسم الأول	الرقم التعريفي
إداري	١٠٠٣٤٥٥	U٨١٢٣٦٥٨	٠٧/٠٥/٩٢	ميرز	سوزان	٠٠٠٠٠٠١
عضو هيئة تدريس	١٠٠٣٤٥٦		٠١/٢٣/٨٨	سمث	جون	٠٠٠٠٠٠٢
طالب		U٧٦٣٤١٠٦	٠٩/١٢/٩٠	جونسون	ديفد	٠٠٠٠٠٠٣

المصادقة الثنائية العوامل:

في النشـــاط التالي ســـنُطبق اســـتخدام (المصادقة الثنائية العوامل). وسوف نقوم ببناء وتثبيت وحدة المصادقة (Google Authenticator) على آلة لينكس الافتراضية والتي سبق الحديث عنها في الفصول السابقة. ووحدة المصادقة (Google Authenticator) عبارة عن تطبيق بكلمة مرور واحدة تعتمد على الوقت، ويعمل هذا التطبيق على الأجهزة المحمولة بنظامـــي آي أو إس (iOS) وآندرويد (Android). وعـــلى الرغم من أنه تم تطوير وحدة المصادقة في الأصل لتوفير (المصادقة الثنائية العوامل) لتطبيقات الشـــبكة المصممة من قبل جوجل، إلا أنه يمكن استخدامها عند تسجيل الدخول إلى نظام لينكس.

ولتثبيت وحدة المصادقة (Google Authenticator) و «su» في حساب الجذر:

```
[alice@sunshine ~]$ su -
Password: thisisasecret
```

قم بنسخ ملفات تثبيت وحدة المصادقة إلى دليل مؤقت، وقم باستخراج الملفات وبناء وحدة المصادقة.

```
[root@sunshine ~]# cp /opt/book/chptr8/
packages/libpam-google-authenticator-
1.0-source.tar /tmp/.
```

```
[root@sunshine ~]# cd /tmp
[root@sunshine /tmp]# tar xvf libpam-
google-authenticator-1.0-source.tar

[root@sunshine /tmp]# cd
libpam-google-authenticator-1.0-source
[root@sunshine libpam…]# make
```

ويجمع الأمر (make) الشـفرة البرمجية إلى مصدر وحدة المصادقة في شـكل إرشادات ثنائية.

بعد ذلك قم بتشغيل الاختبار الآلي:

```
[root@sunshine libpam…]# make test
```

وقم بتثبيت وحدة المصادقة:

```
[root@sunshine libpam…]# make install
```

ولتفعيل الوحدة قم بتعديل الامتداد التالي (/ etc/pam. d/ sshd) ليتوافق مع ما يلي:

```
#%PAM-1.0
auth     required     pam_sepermit.so
auth required   pam_google_authenticator
so nullok.
auth       include       password-auth
account    required     pam_nologin.so
account    include      password-auth
password   include      password-auth
# pam_selinux.so close should be the first
session rule
session  required  pam_selinux.so close
session   required   pam_loginuid.so
# pam_selinux.so open should only be fol-
lowed by sessions to be executed in the
user context
session   required   pam_selinux.so open
env_params
session     optional     pam_keyinit.so
force revoke
session   include   password-auth
```

قم بإعادة تشغيل حارس القشرة الآمنة (Security Shell Daemon (SSHd:

```
[root@sunshine libpam...]# service sshd
restart
```

افتح نافذة طرفية جديدة وقم باستخدام (SSH) للوصول إلى حساب آخر للتأكد من أن الرمز ليس مطلوباً لإدخال شفرة المصادقة وذلك من المستخدمين الذين لم يقوموا بتهيئة وحدة المصادقة (Google Authenticator). ولاختبار ذلك قم بتسجيل الدخول إلى حساب (bob@sunshine) باستخدام (SSH):

```
[alice@sunshine Desktop]$ ssh bob@sunshine
The authenticity of host 'sunshine
(127.0.0.1)' can't be established.
RSA key fingerprint is 5c:40:15:b8:b7:f4:
eb:08:14:cd:1b:c7:d0:4c:76:74.
Are you sure you want to continue con-
necting (yes/no)? yes
Warning: Permanently added'sunshine'
(RSA) to the list of known hosts.
Password: bisforbanana
Last login: Sun May 12 20:23:01 2013 from
sunshine.edu
[bob@sunshine ~]$
```

الآن سنقوم بتهيئة وحدة المصادقة (Google Authenticator) لحساب (bob@sunshine):

```
[bob@sunshine ~]$ google-authenticator
Do you want authentication tokens to be
time-based (y/n) y
https://www.google.com/chart?chs=200x200
&chld=M|0&cht=qr&chl=otpauth://totp/bob@
sunshine.edu%3Fsecret%3DXPE7E73HKJ7S4XB3
Your new secret key is: XPE7E73HKJ7S4XB3
Your verification code is 424105
Your emergency scratch codes are:
  85632437
  55053127
  44712977
  12900353
  82868046
```

احفظ رابط الموقع الناتج عن أمر (google-authenticator) لأنك ستحتاج إليه عند تهيئة الجهاز المحمول الخاص بك.

```
Do you want me to update your «/home/
bob/.google_authenticator» file (y/n) y

Do you want to disallow multiple uses of
the same authentication
token? This restricts you to one login
about every 30s, but it increases

your chances to notice or even prevent
man-in-the-middle attacks (y/n) y

By default, tokens are good for 30 sec-
onds and in order to compensate for
possible time-skew between the client and
the server, we allow an extra
token before and after the current time.

If you experience problems with poor
time synchronization, you can increase
the window from its default
size of 1:30min to about 4min.  Do you want
to do so (y/n) n

If the computer that you are logging into
isn't hardened against brute-force
login attempts, you can enable rate-
limiting for the authentication module.
By default, this limits attackers to no
more than 3 login attempts every 30s.
Do you want to enable rate-limiting (y/n) y
```

الآن تم ضبط وحدة المصادقة (Google Authenticator) لحساب (bob@sunshine) والذي قام بتســجيل الدخول للخادم بـ (SSH). وقبل اختبار الوحدة ســتحتاج إلى تهيئة تطبيق وحــدة المصادقة الخاص بالأجهزة المحمولة بنظام (iOS) أو نظام (Android). أو أنك ســتحتاج إلى اســتخدام واحد من «رموز الشــطب في حالات الطوارئ» (emergency scratch codes) والتي يوفرها أمر (google-authenticator). ويستخدم (تطبيق وحدة المصادقــة الخاص بالأجهزة المحمولــة) طريقة تهيئة مبتكرة حيث يحتوي رمز الاســتجابة السريعــة (QR code) عــلى كل المعلومات المطلوبة لتهيئة الجهــاز المحمول. وقبل تهيئة جهازك المحمول افتــح رابط الموقع الناتج عن أمر (google-authenticator) باســتخدام متصفح جهازك المكتبي وذلك لعرض رمز الاستجابة السريعة الخاص بالتهيئة.

تهيئة وحدة المصادقة (Google Authenticator) على جهاز محمول بنظام (iOS):

ولاستخدام (تطبيق وحدة المصادقة الخاص بالأجهزة المحمولة) يجب أن يكون لديك جهاز آيفون من الجيل الثالث (٣G iPhone) أو أحدث ويكون إصدار نظام (iOS ٥) أو أحدث.

قم بزيارة المتجر الإلكتروني لشركة أبل (Apple App Store).

ابحث عن (Google Authenticator).

قم بتحميل وتثبيت التطبيق.

افتح التطبيق.

انقر على أيقونة زائد.

اضغــط على زر «مســح الباركــود» (Scan Barcode) وقم بتوجيــه الكاميرا على رمز الاستجابة السريعة (الشكل ٨-١٨).

الشكل (٨-١٨): تهيئة رمز الاستجابة السريعة



تهيئة وحدة المصادقة (Google Authenticator) على جهاز محمول بنظام (Android):

ولاســتخدام (تطبيق وحدة المصادقة الخاص بالأجهــزة المحمولة) يجب أن يكون لديك جهاز يعمل بنظام (Android 2.1) أو أحدث.

- قم بزيارة المتجر الإلكتروني لشركة جوجل (Google Play).
- ابحث عن (Google Authenticator).
- قم بتحميل وتثبيت التطبيق.
- انقر على زر «إضافة حساب» (Add an Account).
- اختر «مسح باركود الحساب» (Scan account barcode).

إذا كان التطبيق لا يتمكن من تحديد موقع تطبيق ماسح الباركود على جهازك، سيطلب منك الجهاز تثبيت تطبيق لمسح الباركود. اضغط على زر «تثبيت» (Install) لإنهاء عملية التنصيب.

قم بتوجيه الكاميرا على رمز الاستجابة السريعة.

استخدام وحدة المصادقة (Google Authenticator) على الأجهزة المحمولة:

وبعد أن قمت بتهيئة جهازك المحمول، يمكنك الآن تسجيل الدخول إلى حساب (bob@ sunshine) باســتخدام كلمة المرور ورمز وحدة المصادقة وذلك عبر (SSH). افتح (تطبيق وحدة المصادقة الخاص بالأجهزة المحمولة) مرة أخرى. وســيقدم لك التطبيق رمز مصادقة جديد كل ٣٠ ثانية. وبإمكانك اســتعراض الوقت المُنقضي للرمز الحالي من خلال مشاهدة الدائرة الموجودة في الزاوية اليسرى من الجهة العليا من الجهاز.

```
[alice@sunshine Desktop]$ ssh bob@sunshine
Validation Code: <enter Google
Authenticator code>
Password: bisforbanana
Last login: Sun May 12 22:11:03 2013 from
sunshine.edu
[bob@sunshine ~]$
```

وكـما ترى أن تسـجيل الدخول كان ناجحاً باسـتخدامٍ كلمة المرور ورمـز (تطبيق وحدة المصادقة الخاص بالأجهزة المحمولة). ومن الآن وصاعداً فإنه سـيتم طلب رمز تحقق على جميع محاولات تسـجيل الدخول لحسـاب (bob@sunshine) عـبر (SSH). وإذا كنت ترغب في إيقاف (المصادقة الثنائية العوامل) للحسـاب، ما عليك إلا إزالة ملف (google_authenticator) من الدليل الرئيسي.

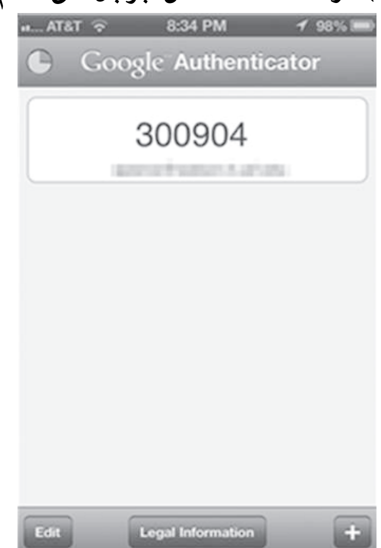
استخدام وحدة المصادقة (Google Authenticator) بدون جهاز محمول:

مـاذا لو فقدت جهازك المحمول أو لم تتمكن مـن الدخول إلى (تطبيق وحدة المصادقة الخاص بالأجهزة المحمولة) (بسبب نفاذ البطارية، أو أن الجهاز مكسور، أو غيرها)؟ في مثل هذه الحالات يتم اسـتخدام «رموز الشـطب في حالات الطوارئ» (emergency scratch codes) والتي يتم إدراجها عند تشـغيل أمر (google-authenticator). ورموز الشـطب هي عبارة عن رموز مصادقة خاصة يمكن استخدامها بدلاً من تطبيق الجهاز المحمول. فإذا وجدت نفسـك يوماً ما بدون جهازك المحمول، بإمكانك اسـتخدام رموز الشطب. ويجب استخدام الرموز بالترتيب الذي تم سردها فيه من أعلى إلى أسفل، كما يمكن أن استخدام كل رمز مرة واحدة فقط (الشكل ٨-١٩). وإذا قمت باستخدام جميع الرموز الخمسة، ستحتاج إلى تشغيل أمر (google-authenticator) مرة أخرى لتوليد رموز جديدة.

سؤال:

العديد من المواقع وخدمات الإنترنت مثل جوجل وتويتر وفيسبوك لديها (مصادقة ثنائية العوامل) لكنها اختيارية. هل تقوم باستخدام أي من تلك الخدمات التي توفر هذا الخيار؟ وإذا كان كذلك، هل تستخدم (المصادقة الثنائية العوامل) مع حسابك؟ علل إجابتك.

الشكل (٨-١٩): وحدة المصادقة من جوجل على نظام (iOS)



تمرين التفكير النقدي - إقطاعية الحلول الأمنية للإنترنت؟

الإقطاعية: النظام الاجتماعي السائد في العصور الوسطى حيث تُمسك طبقة النبلاء بالأراضي من السلطة الملكية في مقابل الخدمة العسكرية، كما يصبح التابعون مستأجرين لدى طبقة النبلاء حيث يتم إجبار الفلاحين (أو العبيد) على العيش في أراضي أسيادهم مع تقديم الإجلال والعمل وحصة من المحصول في مقابل الحماية العسكرية المُفترضة[٢٧].

أشار تمرين التفكير النقدي في الفصل الرابع من هذا الكتاب إلى تفكير مصممي الإنترنت أن الأمن سيكون مسؤولية المستخدم النهائي. ماذا كان مصير هذا التفكير؟ حسناً، لقد تبين أنه من الصعب للغاية بالنسبة للمستخدم النهائي مواكبة المتطلبات الأمنية.

خلال ذروة استخدام الأجهزة الحاسوبية المكتبية، أخذ المستخدم النهائي على عاتقه مسؤولية أمن أجهزة الحاسب الآلي. وقام بعض مزودي خدمات الإنترنت بتقديم اشتراكات مجانية لبرمجيات مكافحة فيروسات بوصفها جزءاً من خدمات الإنترنت المقدمة للمشتركين، لكن مسؤولية الأمن ظلت لدى المستخدم النهائي.

(27) http://www.oxforddictionaries.com

ومع انتشــار الهواتف الذكية والأجهزة اللوحية، تغير هذا النموذج إلى حد كبير في وقت قصــير. ويتوقع المســتخدم النهائي أن أمن الأجهزة متوفر افتراضيــاً ويعمل مباشرة لجميع المســتخدمين. وكــما كتب «بروس شــنير» (Bruce Schneier) في مدونتــه الإلكترونية أن هناك نوعين من التكنولوجيا الحديثة جعلا ذلك أمراً واقعاً: الحوســبة السحابية، والمنصات التي تكون تحت تحكم المورد. وكلما ازدادت شــعبية الحوسبة السحابية، أصبح المزيد من معلوماتنا موجوداً في أجهزة الحاســب الآلي المملوكــة من قبل الشركات بما في ذلك جوجل، وأبل، ومايكروســوفت (المســتندات والبريد الإلكتروني)، وفيســبوك (الصــور). ومن خلال الأجهــزة الذكية، قامت (المنصــات التي تكون تحت تحكم المورد) بتحويل الســيطرة على الأجهــزة الذكية إلى موردي المنصات حيث يتــم التحكم بالهواتف الذكية والأجهزة اللوحية بالكامل تقريباً من قبل الموردين.

وفي هذا العالم حصلنا على مســتويات مرضية جداً من أمن المعلومات، فهناك شــخص يعــرف أكــثر منا يهتم بالأمن، ولكن يتــم تزويدنا بتفاصيل قليلة عن ذلــك، وأحياناً لا يتم تزويدنــا بأي معلومات. لا يمكننا مناقشــة العناصر الأمنية مع هــؤلاء الموردين ولا يمكننا التفــاوض معهم بخصوص الميزات الأمنية. كيف يتم اســتخدام معلومات البريد الإلكتروني في حســاب جوجل أو كيف يتم اســتخدام الصور في حساب فيسبوك؟ المستخدمون عموماً ليس لديهم فكرة عن ذلك. فالمستخدمون لا يستطيعون عرض الملفات أو التحكم بملفات تعريف الارتباط في أجهزتهم اللوحية. وكما كتب «بروس شــنير» (Bruce Schneier) فإن المستخدمين «لديهم رؤية محدودة جداً عن أمن فيسبوك وليس لديهم أي فكرة عن نظام التشغيل الذي يستخدمونه».

وقد أظهر المســتخدمون أنهم يحبون هذه المفاضلة - مزيد من الأمن والراحة في مقابل تحكم محدود على الأمن مع الثقة بأنه ســيتم الوفــاء بالأمن على أكمل وجه. وربما يكون ذلــك صحيحاً من وجهة نظــر الأمن وحده. فالموردون يمكنهم الوفــاء بالأمن أفضل بكثير من مُعظم المســتخدمين النهائيين. النسخ الاحتياطي التلقائي، والكشف عن البرامج الضارة، والتحديثات التلقائية جميعها خدمات أساســية مقدمة بلا تكلفة تقريباً. ومع ذلك وعلى الرغــم من كل هذه الفوائد الضخمة، فإن المســتخدمين في الأصــل على علاقة إقطاعية مع مزودي الخدمات السحابية ومع (المنصات التي تكون تحت تحكم المورد).

وبينـــما كانت العملة في العصر الإقطاعي في العصور الوســطى هـــي (العَمَل)، فإنه في النسخة الحديثة من العصر الاقطاعي العملة هي البيانات. فالمستخدمون يذعنون لشروط مــزودي الخدمة فيما يتعلق بالبيانات، كما يثق المســتخدمون أن الموردين ســيوفرون لهم الأمن. وعندما تصبح الخدمات أكثر تعقيداً مع توفير منافع أكثر، ســيكون هناك اســتدراج أكثر للمســتخدمين لمشــاركة المزيد من بياناتهم مع مزودي الخدمات الســحابية، وذلك لا يشمل البريد الإلكتروني فقط، بل يشمل أيضاً التقويمات ودفاتر العناوين. وإذا كان استيراد تلك البيانات وتصديرها يســتغرق وقتاً ونحن ســعداء مع مزود واحد ومنصة واحدة، فقد نكون على استعداد للثقة الكاملة بمزود واحد.

إذاً مَن هم أســياد الإقطاعية اليوم؟ جوجل وآبل هي أمثلة متعارفة. مايكروســوفت، وفيســبوك، وأمازون، وياهو، وفيرايزون أيضاً من المنافســين على أسياد الاقطاعية اليوم. ما الأوجه الدفاعية لدى المســتخدم ضد التغييرات التعسفية لشروط الخدمة لهؤلاء الموردين؟ نحن نعرف الآن على ســبيل المثال أن جميع هؤلاء الموردين تقريباً يقومون بمشاركة بياناتنا مع الحكومة دون موافقتنا أو إشــعارنا بذلك. فمعظم المســتخدمين يعلمون أن الموردين يبيعون هذه البيانات بهدف الربح، لكن نسبة قليلة من المستخدمين، إن وجدت، يعلمون كيف يتم ذلك، أو لأي غرض، أو بأي شكل.

في العصور الوســطى الأوروبية رهن الناس ولاءهم للســيد الاقطاعي في مقابل الحصول عــلى حمايته. اليوم نحن تطوعنا بولائنا للمزود في مقابل الحصول على حماية هذا المزود. في العصور الوسطى الأوروبية كان الفلاحون يعملون في حقول أسيادهم. اليوم نحن نكدح على مواقعهم الإلكترونية من خلال توفير البيانات والمعلومات الشــخصية (مثل استعلامات البحث، والرسائل الإلكترونية، والإعلانات، والإعجابات).

المراجع:

Schneier. B. «Feudal security:' http://www.schneier.com/blog/archives/2012/12/feudal_sec.html (accessed 07/1412013)

Schneier, B. «More on feudal security,» http://www.schneier.com/blog/archives/2013/06/more_on_feudal.html (accessed 07/14/2013)

أسئلة على تمرين التفكير النقدي:

١. هـــل توافق على أوجه التشـــابه التي كتبها بـــروس شـــنير (Bruce Schneier) بين الإقطاعية في العصور الوســـطى وعلاقة مســـتخدمي التكنولوجية الحديثة بالشركات الكبيرة المزودة للخدمات مثل جوجل وأبل؟

٢. يعتقد بروس شـــنير (Bruce Schneier) أن التدخل الحكومي في عالم تكنولوجيات اليوم هو «الســـبيل الوحيد» لإصلاح علاقة القـــوة غير المتكافئة بين الشركات الكبيرة المقدمة للخدمات والمســـتخدم النهائي. وفي ضوء ما كُشـــف عنه من قيام الحكومة الأمريكية المثير للجدل بمراقبة بيانات مواطني الولايات المتحدة الأمريكية، هل تتفق مع (بروس شنير) في تقييمه لهذا الموضوع؟

٣. هل تعتقد أن السوق الحر يمكن أن يخفف بعضاً من مخاوف بروس شنير؟

تصميم حالة:

في جامعة ولاية الشمس المشرقة، لدى المستخدمين القدرة على استخدام شاشة تسجيل الدخـــول وكلمات المـــرور الخاصة بالجامعة، وذلك لإدارة تســـجيل المقررات الدراســـية في كل فصـــل دراسي. وبعد انتهاء فصل الخريف مبـــاشرة، وبالتحديد بعد انتهاء فترة الحذف والإضافة، تم اســـتدعاؤك إلى مكتب التســـجيل، وذلك للتحقيق في قضية طالبة تشـــكو من حذف جميع مقرراتها الدراسية من النظام، لكنها تدعي أنها لم تقم بذلك.

١. بعـــد قيامك بالبحث عن مفهوم عـــدم التنصـــل (Non-repudiation)، صِف هذا المفهوم.

٢. كيـــف ينطبق هذا المفهوم على المصادقة الإلكترونية وبالخصوص في الحالة المذكورة أعلاه.

بعد إجراء مزيد من التحقيق، اكتشـــفت أن صديق الطالبة السابق، والذي كان منزعجاً من صديقته بســـبب تركها له، اســـتخدم بيانات اعتماد الطالبة الخاصة بالجامعة لتسجيل الدخول إلى النظام وحذف جميع مقرراتها الدراسية.

٣. في اعتقادك كيف حصل صديق الطالبة على بيانات اعتماد حسابها الجامعي؟

٤. كيف يمكن تعديل النظام لاستخدام القياسات الحيوية للتأكد من «عدم التنصل»؟

٥. بالإضافة إلى القياسات الحيوية، ما المقترحات الأخرى المتعلقة بمنهجيات المصادقة، التقنية أو غير التقنية، والتي ستعرضها للتأكد من «عدم التنصل»؟

٦. وبما أن الجامعات تتحرك أكثر فأكثر نحو الدورات الدراسية على الإنترنت، ما الحالات الأخرى التي لا يكون فيها تسجيل الدخول وكلمة المرور كافياً للتأكد من هوية الطالب ولا كافياً كذلك لمنع الاحتيال؟

٧. كيف يمكن للطالبة منع هذه الحادثة؟

الفصل التاسع

الضوابط الأمنية باستخدام المكونات المادية والبرمجيات

نظرة عامة:

في هــذا الفصل ســنُكمل النظرة التفصيلية لمكونات النموذج الأســاسي لأمن المعلومات والــذي تــم عرضه في الفصل الرابع مــن هذا الكتاب. ناقشــنا في الفصل الخامس موضوع تحديد الأصول والتعرف على خصائصها. وفي الفصل الســادس ناقشــنا موضوع التهديدات والثغرات الأمنية. والعنصر الأخير في النموذج الأساسي لأمن المعلومات هو عنصر الضوابط. وفي هذا الفصل سنُلقي نظرة على الضوابط الأكثر أهمية والأكثر شهرة.

في نهاية هذا الفصل يجب أن تعرف ما يلي:

- إدارة كلمات المرور.
- الجُدُر النارية وقُدُراتها.
- قوائم التحكم بالوصول.
- أنظمة كشف/ منع التسلل.
- تصحيحات نظم التشغيل والتطبيقات من الأخطاء.
- حماية نقطة النهاية.
- أفضل ممارسات ضوابط أمن المعلومات.

وليس الغرض من القائمة أعلاه أن تكون شــاملة، بل هي قائمة للضوابط الأساســية التي اختارها مؤلفو هذا الكتاب. ومثال بســيط لأحد الضوابــط الذي لم يُذكر أعلاه هو برنامج مكافحــة الفيروســات. وعلاوة على ذلك فبمجــرد دخولك في مهنة أمــن المعلومات فإنك ســتواجه العديد من ضوابط أمن المعلومات متضمناً ذلك الضوابــط الخاصة بالتطبيقات.

والهدف من الضوابط أعلاه، والهدف كذلك من هذا الفصل عرض الضوابط المعروفة بحيث يكـون لديك فهم للأفكار الأساسـية لضوابط أمن المعلومات. ومعظـم هذه الأفكار قابلة للتعميم لذلك فإنها ستسـاعدك بشـكل عملي على تقييم مزايـا الضوابط التي تواجهها في مستقبلك.

إدارة كلمات المرور:

عرّفنا كلمات المرور بأنها سلسـلة سرية من الرموز التي لا يعرفها سـوى صاحب الهوية والـذي يسـتخدمها لمصادقـة الهوية. وكلمات المرور وسـيلة أمنية مصممة لتكون سـهلة الاسـتخدام للمسـتخدم العادي وأيضاً آمنة لمعظـم التطبيقات. وتُسـتخدم كلمات المرور لحماية البيانات والأنظمة والشـبكات. ويتم عادة الجمع بين اسـم المستخدم وكلمة المرور حيث يعمل اسم المسـتخدم على تحديد الهوية، وتحديد الهوية هو عرض هوية المستخدم على النظام. أما المصادقة فهي تؤسس للثقة في صحة الهوية المُدعاة[1]. فالاستخدام الناجح لاسـم المسـتخدم وكلمة المرور المرتبطة به يوفر للمستخدم الوصول إلى الموارد المقيدة مثل البريد الإلكتروني، والمواقع الإلكترونية، والمعلومات الحساسة وفقاً للأذونات المرتبطة بالهوية.

ولكلمات المرور عدة أسماء مختلفة تبعاً للسياق الذي ترد فيه. فرقم التعريف الشخصي (PIN) هو كلمة مرور عددية قصيرة تتكون من ٤ إلى ٦ أرقام. وتُسـتخدم أرقام التعريف الشـخصية عندما تكـون لوحة المفاتيح الصغـيرة ضرورية (مثل أجهزة الـصرف الآلي)، أو عندما تؤدي كلمات المرور العادية إلى مشكلات مُحتمَلة في سلامة الأفراد (مثل نظام إخماد الحرائق في المطارات). ولأن أرقام التعريف الشـخصية قصيرة فإنه يمكن تخمينها بسـهولة ومن ثم فإن الأمن الذي توفره يكون محدوداً. وبشـكل عام فإن اسـتخدام أرقام التعريف الشخصية مبني على فرضية اسـتخدام آليات أمنية أخرى مثل حد السحب اليومي وكاميرا المراقبة في أجهزة الصرف الآلي، ووسائل الأمن في المطارات.

وشـكل آخر من أشـكال كلـمات المرور هـو عبـارة المـرور (passphrase). وعبارة المـرور هـي سلسـلة مـن الكلـمات التـي تمثـل كلمـة الـسر. مثـلاً العبـارة التالية:

(١) عرّفنا سابقاً المصادقة بأنها «العملية التي يقوم فيها المستخدم بإثبات أنه مالك الهوية التي يستخدمها».

(Wow!!!thisis#1clasatschooL) تمثل عبارة مرور. والدافع وراء استخدام عبارات المرور هو أنه على الرغم من أن المخ البشري يستطيع الاحتفاظ فقط بسبعة أجزاء من المعلومات في الذاكــرة القصــيرة الأجل فإن كل جزء من أجزاء المعلومــات يمكن أن يكون كبيراً إلى حد مــا[٢]. ومــن ثم فإن عبارات المرور يمكن أن تكون أطول من كلمات المرور لكنها أســهل في التذكر من التسلســل العشوائي للرموز. لكن من المهم أن نتذكر أن عبارات المرور البسيطة مثــل (thisisthe#1classatschool) يمكــن تخمينها بســهولة من قبــل المهاجمين مقارنة بكلمات المرور مثل (TiT#`CaS). وليس بالضرورة أن تكون عبارة المرور الطويلة أكثر أمناً من كلمة المرور أو عبارة المرور القصيرة.

ويعتمد أمــن كلمات المرور كلياً على عدم قدرة المهاجمــين على تخمين كلمات المرور. وناقشــنا ســابقاً مجموعتين من المبــادئ التوجيهية لكلمات المــرور. المجموعة الأولى من المبــادئ التوجيهية ترتبط بتعقيد كلمات المرور، أما المجموعة الثانية فترتبط بتنوع كلمات المرور بحيث أن كلمة المرور المسروقة من مورد ما لا يمكن استخدامها في مورد آخر.

والنقاش أعلاه يوضح وجهة نظر المستخدم النهائي بخصوص كلمات المرور: كلمة المرور تسمح لك بالوصول إلى نظام آمن. لكن ولكونك مسؤولاً عن النظام وأخصائي أمن معلومات يتطلــب منــك أن تجعل النظام يعمل، وخاصة أنك مســؤول عن ضمان أمن كلمات المرور التــي تقع تحت عنايتــك، ويتم إنجاز ذلك من خلال إدارة كلــمات المرور. وإدارة كلمات المرور عبارة عن عملية تحديد سياســات كلمات المرور وتنفيذها والحفاظ عليها في جميع أنحــاء المنظمــة[٣]. وإدارة كلمات المرور الفعالة تقلل من احتماليــة اختراق الأنظمة التي تستخدم كلمات المرور.

إدارة كلــمات المرور تعيد تقديم الأبعاد الثلاثة لأمن المعلومات: التكامل (Integrity)، والخصوصية (Confidentiality)، والجاهزية (Availability)، وذلك لأن المنظمات بحاجة

(2) Miller, G.A. «The magical number seven, plus or minus two: some limits on our capacity for processing information,» The Psychological Review, 1956, 63: 81–97, http://www.musanim.com/miller1956/ (accessed 11/1/2012)

(3) NIST Special publication 800-118 (draft), Guide to enterprise password management, http://csrc.nist.gov/publications/drafts/800-118/draft-sp800-118.pdf (accessed 11/1/2012)

لحماية تكامل كلمات المرور وخصوصيتها وجاهزيتها. وباستخدام مصطلحات إدارة الأصول التـي وردت في الفصل الخامس من هذا الكتاب، يمكن النظر إلى كلمات المرور بأنها أصول معلوماتية مقيدة وضرورية. فكلمات المرور أصول مقيدة لأن فقدان الخصوصية أو التكامل يسمح للمهاجمين بالوصول غير المناسب للمعلومات. كما أن كلمات المرور أصول ضرورية لأن عدم جاهزيتها يجعل من الموارد الأساسية المحمية غير متوفرة.

وتعزيزاً لمسـؤوليات المعهد الوطني للمعايير والتكنولوجيـا (National Institute for Standards and Technology) فقـد أصدر مبادئ توجيهيـة للحد الأدنى من التوصيات الخاصة بإدارة كلمات المرور. وسنسـتخدم هذه المبادئ التوجيهية أساسـاً للمعلومات في هذا القسـم. أما المنظمات التي تحتاج إلى متطلبات أمنية أكثر صرامة فبإمكانها أن تفرض اشتراطات إضافية متضمناً ذلك المطالبة بآليات أخرى للمصادقة مختلفة عن كلمات المرور.

وتبـدأ إدارة كلـمات المرور بمعرفة الطرق التي يمكن من خلالهـا اختراق كلمات المرور واتخـاذ إجراءات تقلل من احتمالية وقوع تلـك الاختراقات. وقام المعهد الوطني للمعايير والتكنولوجيا بتحديد أربعة تهديدات لكلمات المرور: التقاط كلمة المرور، وتخمين كلمات المرور وكسرها، واستبدال كلمات المرور، واستخدام كلمات المرور المُخترقة.

تهديدات كلمات المرور:

التقـاط كلمة المرور هو قدرة أحـد المهاجمين على الحصول على كلمة المرور من مكان حفظها، أو أثناء إرسالها، أو من معرفة المستخدم وسلوكه. فإذا تم حفظ كلمة المرور بشكل غـير صحيح في الذاكرة عـن طريق أحد التطبيقات، أو على القـرص الصلب من قبل نظام التشغيل، فإن المستخدم الذي يملك بيانات اعتماد مناسبة قد يتمكن من سرقة كلمة المرور. وبالمثل فإذا لم يتم تشـفير كلمة المرور أثناء إرسـالها، فإنه يمكن الاستيلاء عليها من قبل أي شـخص على الشـبكة. كما يمكن اسـتغلال معرفة المستخدم وسـلوكه من خلال هجمات الهندسة الاجتماعية.

ويُمثـل تخمين كلمة المـرور تهديداً آخر. ففي أثناء تخمين كلمـة المرور يقوم المهاجم بمحاولات متكررة للمصادقة باستخدام كلمات المرور المحتملة مثل كلمات المرور الافتراضية

وكلـمات القاموس. ويمكن أن يتم تخمين كلمات المرور بواسـطة أي مهاجم لديه إمكانية الوصول إلى واجهة تسـجيل الدخول للنظام المستهدف. أما كسر كلمات المرور فهو عملية توليد سلسـلة من الرموز التي تطابق أي سلسـلة من سلاسل كلمات المرور الموجودة على النظام المسـتهدف. ويمكن أن يتم كسر كلمات المرور من خلال المهاجم الذي يتمكن من الوصول إلى الإصدار المشـفر لكلمات المرور المحفوظة. وهذه الإصدارات المشفرة لكلمات المرور تُسمى دوال التجزئة (hashes) وسوف نناقشها في الفصل المتعلق بالتشفير.

أما استبدال كلمة المرور هو استبدال كلمة المرور الحالية للمستخدم بكلمة مرور أخرى لا يعرفها إلا المهاجم. وهذا يحدث عادة من خلال استغلال نقاط الضعف في سياسات النظام الخاصة بإعادة تعيين كلمات المرور وذلك باستخدام مختلف تقنيات الهندسة الاجتماعية.

وكلمات المرور المخترقة هي كلمات مرور موجودة على النظام ويعرفها مستخدمون غير مصرح لهم. وبمجرد أن تُعرف إحدى كلمات المرور فإنه يمكن اسـتغلالها في شـن هجمات الهندسـة الاجتماعية وذلـك لتغيير أذونات الملفات الحساسـة. وإذا كانـت كلمة المرور المخترقة لمسـتخدم بامتيازات عالية، مثلاً مسـؤول النظام، فإن المهاجم قد يكون قادراً على تغيير التطبيقات والأنظمة لاسـتغلالها في وقت لاحق. على سـبيل المثال، قد يكون المهاجم قادراً على إنشاء حساب بامتيازات عالية لنفسه.

وتهتم الإدارة الفعالة لكلمات المرور بهذه التهديدات. وتتمثل توصيات المعهد الوطني للمعايير والتكنولوجيا الخاصة بتدابير إدارة كلمات المرور في صياغة سياسات لكلمات المرور، ومنع التقاط كلمة المرور، ومحاولة التقليل من تخمين أو كسر كلمات المرور، وتطبيق انتهاء صلاحية كلمات المرور كلما تطلب ذلك.

توضح تهديدات كلمات المرور الطبيعة المتكررة لتهديدات أمن المعلومات. وقد ناقشنا فيما سبق تهديدات الأصول. وفي هذا الفصل كنا نحاول تطوير الإجراءات الوقائية ضد التهديدات المشتركة. لكننا وجدنا أن تلك الإجراءات الوقائية نفسها يمكن اختراقها. على سبيل المثال، كلمات المرور هي إجراء وقائي، لكن كلمات المرور يمكن اختراقها، ومن ثم يجب اتخاذ تدابير محددة للحفاظ على أمن الإجراءات الوقائية.

توصيات إدارة كلمات المرور:

سياسات كلمات المرور هي مجموعة من القواعد ذات العلاقة باستخدام كلمات المرور. فبالنسبة للمستخدمين تُحدِد تلك السياسات نوع كلمات المرور المسموح بها. على سبيل المثال، طول كلمات المرور ومدى تعقيدها يندرج تحت هذه الفئة. وبالنسبة لمسؤولي الأنظمة فإن سياسات كلمات المرور تحدد كيف يتم حفظ كلمات المرور، وكيف يتم إرسالها، وكيف يتم إصدارها للمستخدمين الجدد، وكيف يتم إعادة تعيينها إن لزم الأمر. ويجب أن تأخذ (سياسات كلمات المرور) في الاعتبار الأنظمة واللوائح الخاصة بالصناعة التي تعمل فيها المنظمة.

إن الانتباه إلى كيفية قيام كل تقنية في المنظمة بحفظ كلمات المرور من ضروريات تقليل تخمين كلمات المرور وكسرها. فالوصول إلى الملفات وقواعد البيانات المستخدمة لحفظ كلمات المرور يجب أن يكون مقيداً بإحكام. وبدلاً من حفظ كلمات المرور، من المستحسن حفظ دالة تجزئة كلمات المرور (كما وضحنا ذلك بالتفصيل في الفصل السابع). ويجب أن تكون عملية تبادل كلمات المرور مشفرة حتى يستحيل قراءتها أثناء الإرسال. كما يجب التحقق بدقة من هوية جميع المستخدمين الذين يحاولون استعادة كلمات المرور المنسية أو إعادة تعيين كلمات المرور. وأخيراً يجب أن يكون كل مستخدم واعياً لمحاولات سرقة كلمات المرور من خلال هجمات الانتحال، أو من خلال استراق النظر من خلف المستخدم، أو غيرها من الطرق.

ولمنع تخمين وكسر كلمات المرور، يجب أن تكون كلمات المرور معقدة بما فيه الكفاية، كما يتوجب غلق الحسابات التي تواجه العديد من محاولات تسجيل الدخول الفاشلة والمتعاقبة. وهذا يقلل من فرصة القراصنة في تخمين كلمات المرور. كما أن وضع قيود صارمة على الوصول لملفات كلمات المرور وقواعد البيانات التابعة لها يقلل من فرص كسر كلمات المرور.

ويحدد (انتهاء صلاحية كلمة المرور) المدة التي يمكن خلالها استخدام كلمة المرور قبل أن يكون مطلوباً من المستخدم أن يقوم بتغييرها حيث يقلل (انتهاء صلاحية كلمة المرور) من احتمالية استخدام كلمة المرور المخترقة بشكل مُثمر. وعادة يتم جمع كلمات

المــرور مــن خلال إجراءات آلية، مما يســمح بوجود فاصل زمني بــين جمع كلمات المرور وبين قيام المهاجم باســتخدام كلمة المرور المخترقة. فإذا تم تغيير كلمة المرور قبل محاولة المهاجم اســتخدامها، فإن كلمة المرور المخترقة لن تكون ضــارة جداً. لكن (انتهاء صلاحية كلمة المرور) له بعض الســلبيات خصوصاً إذا كانت المنظمة تتطلب كلمات مرور مختلفة لأنظمتها المختلفة. فالمســتخدم ينسى كلمة المرور ومن ثم نحتاج إلى وحدة الدعم الفني، ذات التكلفة العالية، لاســتعادة كلمة المرور المنســية. وبشكل عام يجب استخدام (انتهاء صلاحيــة كلمة المرور) بتعقل من خلال تطبيق فترات زمنية أطول للأنظمة التي تحتاج إلى قليل من الأمان.

قيود كلمات المرور:

بينما تكون كلمات المرور موجودة في كل مكان في مجال أمن المعلومات فإنها تحتوي على الكثير من القيود الهامة. فالمســتخدمون ينسون غالباً كلمات المرور مما يتطلب إما وحدة دعم فني ذات تكلفة عالية للاســتجابة لطلبات المســتخدمين، أو آلية لإعادة تعيين كلمات المرور. لكن آليات إعادة تعيين كلمات المرور تحتوي على بعض الثغرات لأن أسئلة استعادة كلمــة المــرور قد لا تكون قوية بما فيه الكفاية. وفي كثير من الأحيان يحفظ المســتخدمون كلمات المرور في أماكن يستطيع الآخرون رؤيتها. وأخيراً يمكن لهجمات الهندسة الاجتماعية البسيطة نسبياً، مثل الانتحال، أن تكون ناجحة بشكل ملحوظ في سرقة كلمات المرور[٤].

وللأســباب المذكورة أعلاه يتضح أن هنــاك اهتماماً كبيراً في تطوير بدائل لكلمات المرور بهدف المصادقة. لكن الوصول إلى بديل لكلمات المرور ليس بالأمر السهل. فالمستخدمون يعلمون كيفية اســتخدام كلمات المرور والمديرون لا يطلبون من الموظفين تغيير أســاليب العمل إلا للضرورة القصوى. ومما لا يساعد على ذلك محدودية البيانات المتعلقة بالخسائر الفعلية التي تعاني منها المنظمات بسبب سرقة كلمات المرور.

(4) Herley, C. van Oorschot, P.C. and Patrick, A.S. «Passwords: if we're so smart, why are we still using them?» Lecture Notes in Computer Science 5628, 2009, Springer-Verlag

مستقبل كلمات المرور:

وقد تم اقتراح العديد من آليات المصادقة لاستبدال كلمات المرور. وأحد هذه الآليات آلية (Passfaces) والتي يقوم فيها المستخدم بالاختيار المسبق لمجموعة من الوجوه البشرية، وأثناء محاولة تسجيل الدخول يقوم المستخدم باختيار أحد الوجوه من تلك المجموعة. وآلية أخرى هي آلية «رسم السر» (draw-a-secret) والتي يقوم فيها المستخدم برسم خط متواصل عبر شبكة من المربعات. وبينما يكون من المرجح الاستمرار في استخدام كلمات المرور لفترة من الوقت، فإنه لن يكون من المستغرب أن تصبح هذه الآليات أو آليات مماثلة أكثر شعبية في السنوات المقبلة.

> تُعد كلمات المرور والاهتمام العام بإدارة الهوية مجالاً هاماً في الواقع العملي لأمن المعلومات، لذا خصصنا فصلاً كاملاً عن إدارة الهوية وإدارة الوصول في هذا الكتاب.

التحكم في الوصول (Access Control)[5]:

عرّفنا سابقاً التحكم في الوصول بأنه تقييد الوصول إلى موارد نظم المعلومات للمصرح لهم فقط من المستخدمين والبرامج والعمليات والنظم. ونحن نتعامل يومياً مع أنظمة التحكم في الوصول. الأقفال، على سبيل المثال، أحد أشكال التحكم في الوصول. وفي أمن أجهزة الحاسب الآلي يتمثل التحكم في الوصول من خلال استخدام نماذج التحكم في الوصول. ونماذج التحكم في الوصول توضح مدى توافر الموارد في النظام. والنماذج المفيدة في التحكم في الوصول تكون قادرة على تمثيل الحماية المطلوبة للمعلومات والموارد من أي نوع وعلى مستويات متفاوتة من التفاصيل. وفي الوقت نفسه فإن تنفيذ النماذج ينبغي ألا يضع حملاً مفرطاً على القدرات الحاسوبية لنظام التشغيل. وهناك طريقتان شائعتان لتطبيق نماذج التحكم في الوصول وهما: قوائم التحكم في الوصول (access control lists)، والتحكم في الوصول المعتمد على الدور (role-based access control).

(5) Tolone, W. Gail-Joon Ahn and Tanusree Pai, «Access control in collaborative systems,» ACM Computing Surveys, 37(1): 29–41

قوائم التحكم في الوصول (Access Control Lists) (ACLs):

قائمــة التحكم في الوصول هــي قائمة من الأذونات تتبع مكونات محددة. وتســتخدم قوائم التحكم في الوصول جُمَلاً بسيطة لتحديد الأشخاص (subjects) والمكونات (objects) والعمليات المسموح بها. على سبيل المثال، إذا كانت قائمة التحكم في الوصول لاتصال بالشبكة تنص عــلى (ANY, block ,131.247.93.68)، فإنه يجب منع المضيف (١٣١,٢٤٧,٩٣,٦٨) من المرور عبر الاتصال بالشبكة أو الوصول إلى أي مورد على الشبكة. ويقوم نظام التشغيل بالتحقــق من طلبات الموارد الواردة بهــدف معرفة مدخلات قائمة التحكم في الوصول التي قد تمنع الوصول إلى الموارد.

وتُســتخدم قوائــم التحكــم في الوصول عادة للدفــاع عن نوعين من المــوارد: الملفات واتصالات الشــبكات. وتقوم (قوائم التحكم في الوصول لحمايــة الملفات) بتحديد حقوق المســتخدمين، سواء كانوا أفراداً أم جماعات، وذلك للوصول إلى الملفات والملفات التنفيذية. واستخدام أمر (chmod) في الفصل الثالث هو أحد أمثلة (قوائم التحكم في الوصول لحماية الملفــات). وتقوم (قوائم التحكم في الوصول لحماية اتصالات الشــبكات) بتحديد القواعد لمعرفة أرقام المنافذ والعناوين الشــبكية التي يمكن الوصول إليها. وتُعد (قوائم التحكم في الوصول إلى حماية اتصالات الشبكات) أحد الطرق الشائعة في تطبيق الجُدُر النارية (والتي سنناقشها لاحقاً في هذا الفصل). ومعظم أنظمة التشغيل الحديثة تأتي بقوائم تحكم وصول افتراضية والتي توفر مستويات معقولة من الأمن للمستخدم العادي. وتُعد قوائم التحكم في الوصول من أبســط الضوابط في التطبيق، كما تعتمد فاعلية العديد من الضوابط الأمنية الأخرى على قوائم التحكم في الوصول. على ســبيل المثال، تساعد قوائم التحكم في الوصول إلى المحافظة على تكامل وجاهزية كلمات المرور عن طريق منع المهاجمين من الكتابة فوق كلمات المرور.

وتبدأ قوائم التحكم في الوصول من الفرق الأساسي بين الأشخاص والمكونات. فالأشخاص يحاولــون تنفيذ العمليــات على المكونات، ويتم الســماح بتنفيذ العمليــات إذا كان ذلك مســموحاً مــن قبل قوائم التحكــم في الوصول. ويمكــن تمثيل قوائم التحكــم في الوصول باعتبارها (مصفوفة وصول) تقوم بتحديد الأذونات لكل شــخص وعلى كل مكون. ويوضح

الشكل (٩-١) مثالاً على ذلك. وتوضح كل خلية في الصورة أذونات الوصول للشخص المقابل والمستخدم للمكون المقابل.

الشخص جون (John) هو مالك الملف رقم (١)، كما أن لديه أذونات قراءة وكتابة على الملــف. ولأن جون (John) مالك الملف يمكنه تعيين أذونات على الملف لأي شــخص. وفي هذه الحالة تم إعطاء الشخص بوب (Bob) إذن قراءة الملف، كما تم إعطاء الشخص أليس (Alice) إذن التنفيــذ على الملــف. وهكذا فإن كل خلية تمثل قائمة تحكم في الوصول لكل مستخدم للمكون المقابل.

الشكل (٩-١): مثال على مصفوفة وصول

		المكونات		
		Host 1	File 1	File 2
الأشخاص	John	حظر	مالك قراءة كتابة	قراءة
	Bob	حظر	قراءة	قراءة
	Alice	سماح	تنفيذ	مالك قراءة كتابة تنفيذ

القيود:

تُعد قوائم التحكم في الوصول آلية بسيطة جداً لكنها فعالة لمراقبة الوصول. ومع ذلك فهــي لا تخلو من بعــض القيود الهامة. فإذا كان يجب تعديل الأذونات لمســتخدم معين، فإنه يجب تعديل الأذونات على جميع المكونات التي يتمكن هذا المســتخدم من الوصول إليها. وأيضاً فإنه ليس من الممكن تعيين أذونات على أســاس مســؤوليات المستخدم. فإذا تم تغيير دور المســتخدم فإن منح أذونات الوصول المناســبة للدور الجديد لهذا المستخدم يتطلب تعديل الأذونات لكل مستخدم على حدة، وذلك على جميع المكونات ذات العلاقة.

التحكم في الوصول المُعتمد على الدور (Role-Based Access Control) (RBAC):

لقد رأينا أن (التحكم في الوصول المُعتمد على الدور) يُعين الأذونات للمســتخدمين بناءً على الدور بدلاً من تعيينها بناءً على المستخدم الفردي حيث يتم إنشاء الأدوار لمهام العمل، ويتم تعيين الأدوار للمستخدمين بناءً على مسؤولياتهم. ومن خلال تحديد أذونات الوصول لــلأدوار، هناك فرق بين ضوابط المســتخدم، وضوابط الوصول. فالمســتخدمون يتطورون تدريجياً في المنظمة، أدوارهم يمكن تعيينها، وأذونات الوصول يتم تحديثها تلقائياً. لذا عند مقارنــة (التحكم في الوصول المُعتمد على الدور) بـــ (قوائم التحكم في الوصول) فإن الأول يقلــل من التكاليف ومن الجهد الإداري المطلوب لتنفيــذ التحكم في الوصول في المنظمات الكبيرة.

الجُدُر النارية[٦]:

الجُدُر النارية هي شــكل من أشــكال الحماية التي تسمح لشــبكة ما بالاتصال بشبكة أخرى مع الحفاظ على مستوى معين من الحماية. وأحد أكثر الأمثلة المألوفة لجُدُر الحماية هــو باب المنزل أو المكتب. فالباب يســمح للســكان بالخروج من المنــزل لكنه يمنع المطر والصقيع من الدخول للمنزل. كما يســاعد البــاب أيضاً في الحفاظ على قدر من خصوصية السكان.

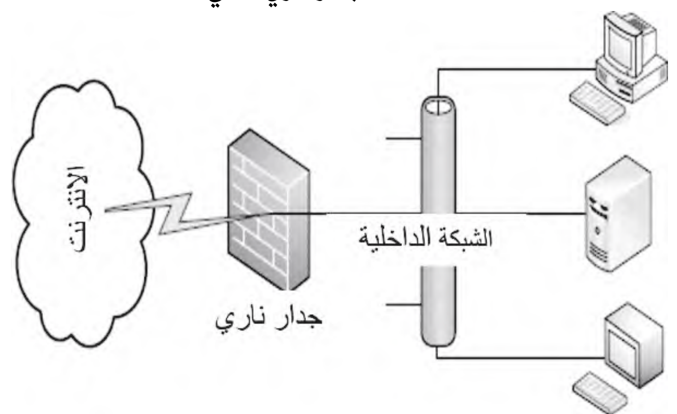
الجُدُر النارية للشبكات هي مكونات مادية أو برمجية تمنع الأخطار التي تنشأ في شبكة ما من الانتشــار إلى شــبكة أخرى. وفي الواقع العملي فإن الجُدُر النارية للشــبكات تقوم بأغراض متعددة بما في ذلك (١) تقييد الدخول والخروج من الشــبكة، وذلك لمواقع محددة بدقــة، و(٢) الحــد من حركة المرور عــلى الإنترنت وذلك لتطبيق معــين يعمل على أجهزة معينــة، و(٣) منع حركــة المرور الصادرة من المُضيف الذي يُشــتبه باختراقه. وعموماً فإن الجُدُر النارية ليست مُعدة للدفاع عن هجمات مخصصة. فأبواب متاجر بيع التجزئة، على ســبيل المثال، ليست مصممة للكشف عن المتسوق الذي يحمل متفجرات، أو عن المتسوق

(٦) المصدر التالي مصدر ممتاز عن الجدر النارية للإنترنت، «Building Internet firewalls,» by Elizabeth D. Zwicky, Simon Cooper and D. Brent Chapman, O' Reilly Media, ISBN 978-1-56592-871-8 (896 pages). وكثير من معلومات هذا القسم تستند على هذا المصدر.

الســارق. فتلك المهام، إذا كانت ضرورية (في المطارات على سبيل المثال) تُترك لضوابط أكثر تخصصــاً مثل المفتش البشري أو تقنيات الحماية ضد السرقة. ومع ذلك فإن الجُدُر النارية تُعد خط الدفاع الأول الفعال وغير المكلف نسبياً ضد عدد كبير من المضايقات الشائعة.

ويوضح الشكل (٩-٢) الترتيب الشائع لجدار حماية يقع بين الشبكة الداخلية للمنظمة والشــبكات الخارجية مثل الإنترنت. ويتم توجيه حركة المرور بين الإنترنت وشبكة المنظمة الداخلية من خلال الجدار الناري حيث يمكن تنفيذ قواعد مرور المنظمة.

الشكل (٩-٢): جدار ناري نمطي



قرارات الجُدُر النارية:

أمــام الجدار الناري أحــد الخيارين بخصوص الحزم التي تمر عبره -الســماح أو الرفض. فالحزم المســموح لها تواصل وجهتها المقصودة، بينما الحزم الممنوعة يتم حظرها في الجدار النــاري. ونبدأ بالحالة الأساســية للجدار الناري: الرفض الافتراضي، أو الســماح الافتراضي. فإذا كانت الحالة الأساسية للجدار الناري هي السماح الافتراضي فإنه سيسمح لجميع الحزم في الشبكة باستثناء تلك المحظورة صراحة. أما إذا كانت الحالة الأساسية للجدار الناري هي الرفض الافتراضي فإنه سيحظر جميع الحزم في الشبكة باستثناء تلك المسموح بها صراحة.

الرفض الافتراضي أم السماح الافتراضي؟

توصية الأمان الموحدة هي استخدام حالة الرفض الافتراضي. وبهذه الطريقة فإن الخدمات المعروف أنها آمنة فقط ستكون قابلة للوصول للإنترنت. لكن المستخدم يفضل عادة حالة السماح الافتراضي لأنها تتيح للخدمات التجريبية وغيرها من خدمات الإنترنت أن تعمل.

ويمكن لحالة السماح الافتراضي أن تكون مقبولة للإداريين والطلاب الذين يتعلمون كيفية تهيئة الجُدُر النارية. وأما بالنسبة لجميع الاستخدامات الأخرى فيُفترض اعتماد حالة الرفض الافتراضي.

ويتم تعزيز الحالة الأساسية للجُدُر النارية من قبل المسؤول الذي يخصص قواعد لقوائم التحكم في الوصول (ACL)، وذلك لتحديد الحزم المسموح بها (على فرض أنه تم اعتماد حالة الرفض الافتراضي). وبعض القواعد الممثلة لهذه الحالة موضحة أدناه باستخدام برنامج (ipfilter)، وهو برنامج جداري ناري شائع الاستخدام.

```
pass in quick from 192.168.1.024/ to 192.168.10.50
pass out quick from 192.168.10.50 to 192.168.1.024/
pass in log quick from any to any port = 22
pass out log quick from any port = 22 to any
block in all
block out all
```

ويمكن تفسير هذه القواعد على النحو التالي: القاعدتان الأولى والثانية تسمحان بالوصول والمغادرة من عنوان بروتوكول الإنترنت «أو عنوان بروتوكول الإنترنت (IP address)» (١٩٢,١٦٨,١٠,٥٠) إلى أي عنوان بروتوكول الإنترنت في الشبكة الفرعية (٢٤/١٩٢,١٦٨,١,٠). وهذا العنوان (٢٤/١٩٢,١٦٨,١,٠) هو وسيلة مدمجة لتمثيل جميع عناوين بروتوكول الإنترنت من (١٩٢,١٦٨,١,٠) إلى (١٩٢,١٦٨,١,٢٥٥). ويمكن أن يكون هذا مفيداً إذا تم، على سبيل المثال، استخدام المضيف (١٩٢,١٦٨,١٠,٥٠) لتوفير خدمات مشتركة مثل مشاركة الملف أو مشاركة الطابعة، أو لتوفير بوابة إلكترونية للمشاركة (Sharepoint portal) في المنظمة. أما المجموعة الثانية من القواعد فتُتيح لجميع الاتصالات الواردة والصادرة خدمة «ssh» (وهي خدمة تسجيل الدخول عن بعد لمضيف نظام ينكس). كما تُحدد قواعد

(SSH) بأن جميع معاملات (ssh) سـيتم تسـجيلها. وقد ترغب المنظمة في فعل ذلك من أجل تتبع جميع أنشطة (SSH). أما القاعدتان الأخيرتان فتحددان الحالة الافتراضية للجدار الناري، وهي حالة الرفض الافتراضي.

قيود الجُدُر النارية:

نظـراً لرواج اسـتخدام الجُدر النارية، من المهم أن نعرف ما لا تسـتطيع الجدر النارية القيام به. وبعض القيود الهامة للجُدُر النارية تشمل ما يلي:

الأعضـاء الداخليـون وحركة المرور غير المنظمـة: الجُدر النارية تحمـي المنظمة من الهجمات التي تأتي من خارج الشبكة. فإذا تم اختراق جهاز حاسب آلي داخل المنظمة، فقد يتمكـن المُخترِق مـن سرقة البيانات من أجهزة الحاسـب الآلي الأخرى داخل المنظمة دون المرور عبر الجُدر النارية. وبالمثل فإذا أحضر شخص ما جهاز التخزين المحمول (فلاش) وقام بنسـخ البيانات الحساسة على ذلك الجهاز، فلا تستطيع الجُدر النارية القيام بأي شيء لمنع هذه السرقة لأن حركة مرور البيانات لا تمر من خلال الجُدر النارية.

حركة المرور المشفرة: لا يمكن فحص البيانات المشفرة، ومن ثم فإن لدى الجُدر النارية قدرة محدودة في الدفاع عن البيانات المشفرة. على سبيل المثال، إذا قام المستخدم بتصفح موقـع آمن، فـإن الجدار الناري لن يكون قـادراً على فحص المعلومات المشـفرة التي يتم تبادلها بين المستخدم والموقع الإلكتروني.

التهيئـة: إن أمن الجُدر النارية وسـهولة اسـتخدامها يعتمدان عـلى تهيئتها من قبل مسؤول النظام. فالجُدر النارية المُهيئة بشكل ضعيف تكون أكثر عرضة لحركة المرور الضارة ومن ثم الوصول إلى أهداف حساسـة. وفي الوقت ذاته يُعد الأمن الذي تمنحه تلك الجُدُر النارية أمناً كاذباً.

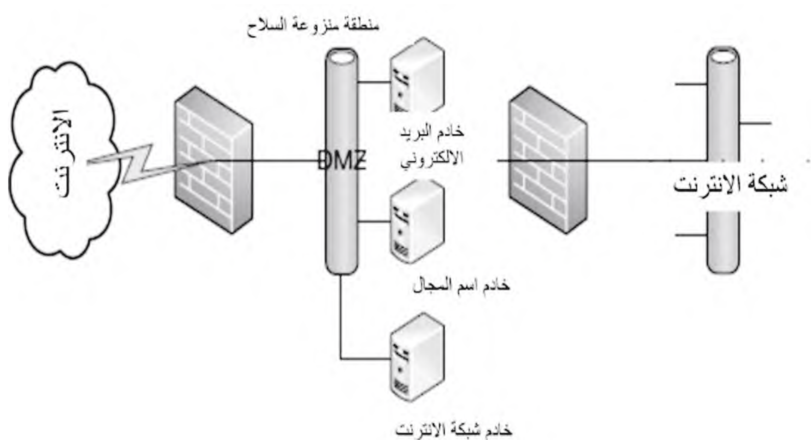
أنواع الجُدُر النارية:

بشـكل عام هناك نوعان من الجُـدُر النارية: جُدُر نارية لتصفيـة الحُزم، وجُدُر نارية للفحـص العميق للحزم. وتقوم (الجُـدُر النارية لتصفية الحُزم) بفحـص الحقول العلوية

لبروتوكول الحزم التي تتدفق من خلال الجدار الناري لتحديد ما إذا كان سيُسمح للحزمة بالدخول إلى الشبكة. وقد تقوم (الجُدُر النارية لتصفية الحُزم) بفحص الحقول مثل عناوين بروتوكول الإنترنت التابعة للمصدر وللوجهة، وعناوين منفذ الوجهة، وإشارات بروتوكول التحكم بالنقل (TCP flags). وأحد استخدامات هذا النوع من الجُدُر النارية هو حظر الحزم الواردة من مضيف أو من مزود خدمة الإنترنت والذي لديه تاريخ في إرسال كميات كبيرة من رسائل البريد المزعجة. ويمكن تحديد المضيف أو مزود خدمة الإنترنت من خلال حقل عنوان بروتوكول الإنترنت التابع للمصدر.

أما (الجُدُر النارية للفحص العميق للحزم) فتقوم بفحص البيانات التي تحملها الحزمة، بالإضافة إلى فحص الحقول العلوية لبروتوكول الحزم، وذلك لاتخاذ قرار بشأن كيفية التعامل مع الحزمة. ويمكن مقارنة البيانات التي تحملها الحزمة بقاعدة البيانات التي تحتوي على الحُمولات الخبيثة المعروفة. ويمكن التعرف من خلال هذه المقارنة على محاولات إطلاق هجمات (تجاوز سعة المخزن المؤقت) أو الهجمات الأخرى التي تعتمد على الحُمولات التي تمت صياغتها بعناية.

الشكل (٩-٣): الجُدُر النارية المحيطة والمناطق منزوعة السلاح



تنظيم الجُدُر النارية:

الشــكل (٩-٢) هو تمثيل مبسط لكيفية استخدام الجُدُر النارية. أما الشكل (٩-٣) فهو يوضح التهيئة القياســية للجدار الناري. وهذا الشــكل يحتوي على محيط الجدار الناري، والمنطقة المنزوعة السلاح، والجدار الناري الداخلي، والمنطقة المُسلحة.

محيــط الجــدار الناري هو جدار الحمايــة الذي يقع بين الشــبكة الخارجية والمنظمة. ويســمح هــذا المحيط للمُضيف خــارج المنظمة أن يصــل إلى الخدمــات الموجهة للعامة والخدمات المقدمة من قبل المنظمة مثل شــبكة الإنترنت، والبريد الإلكتروني، ونظام اســم المجال (DNS).

الشبكة المحيطة، والتي تسمى أيضاً المنطقة المنزوعة السلاح، هي الشبكة التي تقع بين الشبكة الخارجية والشبكة الداخلية للمنظمة. وتقوم الشبكة المحيطة باستضافة الخدمات الخارجيــة مثل بروتوكول انتقال النص التشــعبي (http)، وبروتوكول نقل البريد الإلكتروني (smtp)، ونظام اسم المجال (DNS).

الشبكة الداخلية، أو المنطقة المُسلحة، هي موقع جميع الأصول المعلوماتية للمنظمة.

إن الجــدار الناري الداخلي يُقيد الوصول لشــبكة المنظمة الداخلية. وبشــكل عام فإن الوصول لشــبكة المنظمة الداخلية يقتصر على بعــض التطبيقات المعينة بناءً على الطلبات القادمــة من المُضيف المحدد على الشــبكة المحيطة. على ســبيل المثــال، بإمكان الجامعة أن تحافــظ عــلى بوابــة إلكترونية في المنطقة منزوعة الســلاح. لكن الموارد مثل ســجلات الطلاب تكون محفوظة في الشبكة الداخلية، ويمكن الوصول إلى هذه الموارد فقط باستخدام الطلبات التي تنشــأ من البوابة الإلكترونية. وإذا تم اختراق البوابة، فإن المعلومات الأخرى داخل الجامعة ليست معرضة للاختراق.

التوصيات الأساسية للجُدُر النارية

إذا كنت مكلفاً بوضع إعدادات جدار الحماية التابع لمنظمة صغيرة أو لإدارة ما، تجد هنا بعض الإعدادات التي يمكنك البدء بها. وبشكل عام اسمح للمستخدمين بالوصول إلى الخدمات التالية على شبكة الإنترنت:

الإنترنت (منفذ ٨٠، ٤٤٣) لمضيف محدد يشغل خوادم الإنترنت.
البريد الإلكتروني (منفذ ٢٥، ٤٦٥، ٥٨٥، ٩٩٣، ٩٩٥) لمضيف محدد يشغل خوادم البريد الإلكتروني.
نظام اسم المجال (منفذ ٥٣) لمضيف محدد يشغل خدمة نظام اسم المجال.
التواصل عن بعد لأجهزة سطح المكتب (منفذ ٣٣٨٩).
خدمة تسجيل الدخول عن بعد (SSH) (منفذ ٢٢) لمضيف معين بنظام ينكس.

والقاعدة العامة هنا هي السماح للخدمات الآمنة، وهي الخدمات الشائعة الاستخدام والتي تقوم بتشفير المعاملات. ويعد شيوع استخدام الخدمة مهماً، وذلك لضمان أن البرمجيات ذات الصلة يتم تحديثها باستمرار عند الإبلاغ عن أي ثغرة أمنية. وأكثر تلك الخدمات شيوعاً هي خدمة تسجيل الدخول عن بعد (SSH) (لنظام ينكس) وخدمة التواصل عن بعد لأجهزة سطح المكتب (لعملاء ويندوز). وفي أي مؤسسة تجارية تقليدية، يُسمح عادة لهذه الخدمات بالاتصال بأي مضيف سواء كان داخل الشبكة أم خارجها.

وهناك مجموعة أخرى من الخدمات تسمى بالمجموعة الآمنة. وهذه الخدمات الشائعة يمكن استخدامها كما هو محدد، لكن لا يتم تشفير معاملاتها. ومن أمثلة هذه الخدمات البريد الإلكتروني وشبكة الإنترنت. ولهذه الأسباب من المستحسن أن يُسمح للمضيف فقط بالاتصال بخوادم الإنترنت أو خوادم البريد الإلكتروني على المضيف الذي يُدار من قبل مسؤول نظام مدرب وموثوق به. وهذا يضمن أنه حتى في حال كانت خوادم الإنترنت مُفعلة عن طريق الخطأ بواسطة مستخدم ما ولم يتم تحديثها بعد ذلك، فإن الخطر الذي تشكله هذه الخوادم يكون محدوداً.

ومن الخدمات الشائعة الاستخدام في السابق لكنها فاقدة للثقة اليوم هي خدمة بروتوكول تلنت (Telnet) وخدمة بروتوكول نقل الملفات (FTP). وهذه الخدمات تم استبدالها بنظيرها الآمن وهي (خدمة تسجيل الدخول عن بعد-SSH) لأن تلك البرمجيات لا تجري صيانتها مما ترك مجالاً لثغرات محتملة. وبشكل عام يجب حظر تلك الخدمات ما لم يكن هناك سبب خاص لتفعيلها (مثلاً السماح للتطبيقات القديمة باستخدامها حتى تتمكن من العمل).

والأشــكال التالية توضح الجدار الناري لويندوز أثناء عمله. فالعمود الأيسر يوضح قيام الجدار الناري بحظر طلبات بروتوكول انتقال النص التشعبي (http)، لأن الموقع الإلكتروني الــذي يعمل على المضيف لا يمكن الوصول إليه من العالم الخارجي. والعمود الأيمن يوضح المضيف نفســه لكن تم تهيئة الجدار الناري لويندوز بالســماح لطلبــات بروتوكول انتقال النص التشــعبي (http) حيث يمكن الآن الوصــول إلى الموقع الإلكتروني من العالم الخارجي (الشكل ٩-٤، والشكل ٩-٥).

أنظمة كشف/منع التسلل:

تتعرض أنظمة تقنية المعلومات لهجوم مســتمر من مصادر مختلفة. على سبيل المثال، أفادت الوكالات الفدرالية أن عدد الحوادث الأمنية التي جعلت المعلومات الحساســة على الأنظمــة الفدرالية في خطر قد زادت من ٥٥٠٣ في عام ٢٠٠٦ إلى ٤١٧٧٦ في عام ٢٠١٠، أي بزيــادة قدرها أكثر مــن (٦٥٠٪) خلال هذه الفترة[٧]. وللاســتجابة الفعالة لهذه الحوادث فقد اهتم مسؤولي الأنظمة بالتكنولوجيا التي تستطيع اكتشاف محاولات التسلل في الوقت الفعلي وتقوم بتنبيه مسؤولي الأنظمة حتى يتمكنوا من الاستجابة بسرعة. وقد أدت هذه الحاجة إلى تطوير أنظمة كشف التسلل.

أنظمــة كشــف التســلل (Intrusion detection systems) أو اختصــاراً (IDS) هي مكونــات مادية أو تطبيقات برمجية تراقب أنظمة تقنية المعلومات لاكتشــاف الأنشــطة الضارة أو اكتشــاف انتهاكات سياســات الاستخدام التي أُنشــئت من قبل مسؤول النظام. أما أنظمة منع التســلل فيتم بناؤها على أنظمة كشــف التســلل بهدف إيقاف الاختراقات المحتملة. وقد أصبحت الآن أنظمة كشــف التســلل وإلى حد ما أنظمة منع التســلل أيضاً جزءاً لا يتجزأ من البنية التحتية لأمن تقنية المعلومات في معظم المنظمات.

وبشــكل عام هناك نوعان من أنظمة كشــف التســلل: أنظمة معتمدة على الشــبكة، وأنظمة معتمدة على المضيف. أنظمة كشــف التسلل المعتمدة على الشبكة تراقب حركة

(7) INFORMATION SECURITY: Weaknesses Continue Amid New Federal Efforts to Implement Requirements, United States Government Accountability Office, GAO Report to Congressional Committees, GAO-12-137, October 2011, http://www.gao.gov/assets/590/585570.pdf (accessed 11/23/2012)

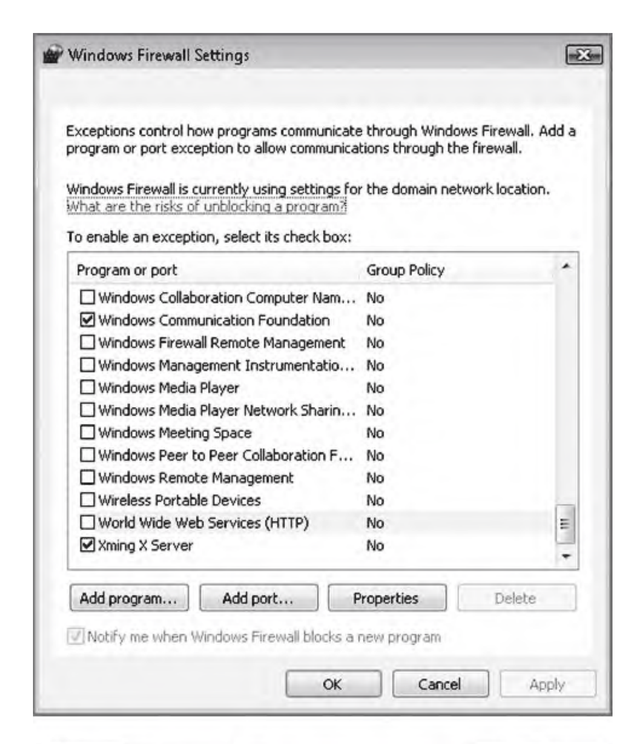
مرور الشبكة ونشاط بروتوكول التطبيقات لتحديد الاتصالات المشبوهة. وتأتي هذه الأنظمة عادة مع الموجهات والجُدُر النارية[٨]. أما أنظمة كشف التسلل المعتمدة على المضيف فهي تطبيقات برمجية مُثبتة على المضيف الذي يراقب النشـاط الداخلي مثل الوصول للملفات واسـتدعاء الأنظمة بهدف اكتشاف الأنشطة المشبوهة. ولزيادة احتمالية كشف محاولات التسلل، تقوم معظم المنظمات بالاستفادة من العديد من أنظمة كشف التسلل، ولكلٍ منها مجموعة من القواعد المحددة وذلك لمراقبة نشاط النظام من وجهة نظرها الخاصة.

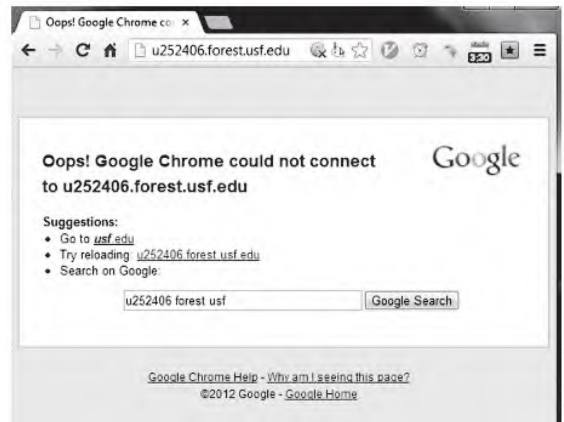
وأحد وظائف (أنظمة كشف التسلل) المثيرة للاهتمام هو إطلاق الإنذارات حول الهجمات الوشـيكة. ويتم ذلك من خلال مشاهدة نشاط الاستطلاع: مسح المنافذ والمضيف لتحديد أهداف الهجمات اللاحقة. وهذا المسح غالباً ما يسبق الهجمات ذات النطاق الواسع، وإذا تم إخطار مسـؤول النظام بعمليات مسـح المنافذ، فإنه يسـتطيع اتخاذ الإجراءات اللازمة للاستعداد لأي هجمات قادمة.

---

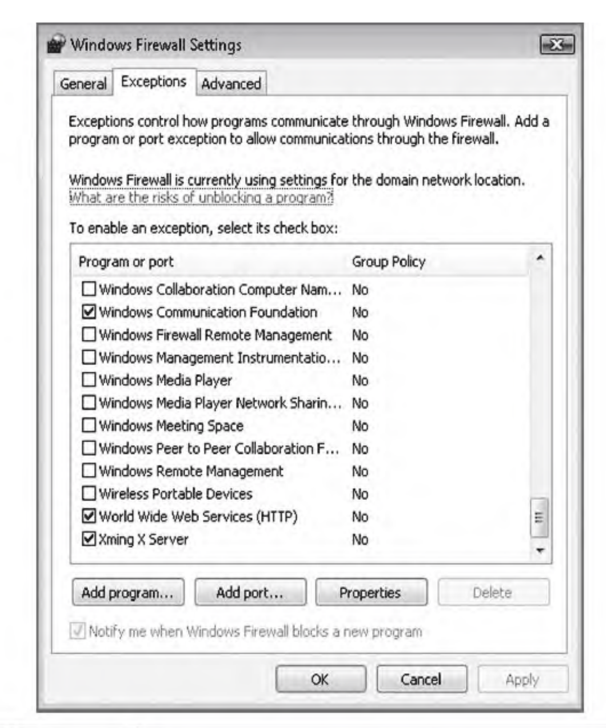
(8) Karen Scarfone and Peter Mell, NIST Guide to Intrusion detection and prevention systems, 800 publication special-94, 800/nistpubs/publications/gov.nist.csrc://http-94/SP800-94.pdf (accessed 11/23/2012). The National Institute of Standards and Technology (NIST) includes two other categories of IDS – wireless and network behavior analysis (NBA). (وقد أضاف المعهد الوطني للمعايير والتكنولوجيا نوعين آخرين لأنظمة كشف التسلل هي اللاسلكية وتحليل سلوك الشبكة. ولأهداف هذا الفصل، فإن هذين النوعين يندرجان تحت أنظمة كشف التسلل المُعتمدة على الشبكة. وهذا الدليل هو مصدر كثير من معلومات هذا القسم حول أنظمة كشف/منع التسلل).

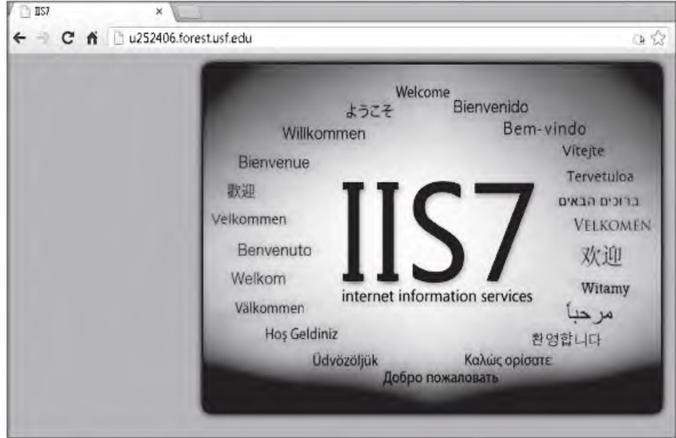
الشكل (٩-٤): الجدار الناري لويندوز وهو يحظر بروتوكول انتقال النص التشعبي (http)





الشكل (٩-٥): الجدار الناري لويندوز وهو يسمح لبروتوكول انتقال النص التشعبي (http)





طُرق الاكتشاف:

تعتمد أنظمة كشف التسلل المعاصرة على ثلاث طرق: التوقيعات، والانحرافات، وحالات البروتوكول. وتســتخدم معظم التطبيقات التجارية مزيجاً من الطرق الثلاثة لتحقيق أقصى قدر من الفعالية.

أنظمة كشف التسلل المُعتمدة على التوقيعات:

التوقيع هو سلســلة من البايتات المعروف عنها أنها جزء من البرمجيات الضارة. وتقوم (أنظمة كشف التسلل المُعتمدة على التوقيعات) بمقارنة الأحداث المرصودة بقاعدة بيانات التوقيعــات وذلك لتحديد الحوادث المحتملة. ومن أمثلة التوقيعات الرســائل الإلكترونية التي عنوانها (ILOVEYOU) وتحتوي على ملف مرفق باسم (LOVE-LETTER-FOR-YOU.txt.vbs). وهذه الرســائل الإلكترونية تتوافق مع فيروس (ILOVEYOU) المعروف والذي أُصدر في الفلبين في تاريخ ٥-٥-٢٠٠٠.

وتُعد (أنظمة كشــف التســلل المُعتمدة عــلى التوقيعات) فعالة جــداً ضد التهديدات البســيطة والمعروفة. وحســابياً فإن هــذه الأنظمة فعالــة جداً لأنها تســتخدم عمليات مقارنة السلاســل البســيطة. لكن هذه الأنظمة غير مفيدة في الكشف عن التهديدات غير المعروفة سابقاً، أو التهديدات المتنكرة، أو التهديدات المعقدة. على سبيل المثال، إن فيروس (ILOVEYOU) يكــون فعالاً بالقدر نفســه عند تغيير عنوان رســالة البريد الإلكتروني إلى (job offer for you) وتغيير اســم الملف المرفق إلى (interview-script.vbs). لكن هذا التنكر البسيط يجعل اكتشاف الفيروس أمراً صعباً للغاية بالنسبة لـ (أنظمة كشف التسلل المُعتمدة على التوقيعات).

والعيــب الآخر في (أنظمة كشــف التســلل المُعتمدة على التوقيعــات) هو أن مطابقة التوقيع يقتصر فقط على الوحدة الحالية من النشــاط، مثلاً حزمة واردة أو إدخال ســجل فــردي. وهــذه الأنظمة لا تفهم عمليات بروتوكولات الشــبكة. ونتيجــة لذلك لا يمكن لـ (أنظمة كشــف التسلل المُعتمدة على التوقيعات) اكتشــاف عمليات مسح المنافذ لأن كل حزمة فردية يتم فحصها تمثل حزمة مشروعة ويتم تشــكليها بشكل جيد. ويتطلب كشف

التهديد لعمليات مسح المنافذ تجميع المعلومات عن الحزمة الحالية، ومعلومات عن الحزم التي تم استقبالها في الماضي، ولا تستطيع مطابقة التوقيعات للحزمة الحالية لوحدها القيام بهذا الأمر. وبشـكل عام فإن (أنظمة كشف التسلل المُعتمدة على التوقيعات) لا تستطيع كشـف الهجمات التي تتألف من أحداث متعددة، وذلك إذا كان أي من الأحداث الفردية لا يتطابق بشكل واضح مع توقيع هجوم معروف.

أنظمة كشف التسلل المُعتمدة على الانحرافات:

(أنظمة كشـف التسـلل المُعتمـدة على الانحرافـات) هي عبارة عن عملية الكشـف عـن الانحرافـات بين الأحداث المُلاحظة وأنماط النشـاط المحدد. ويحدد مسـؤول النظام أوضاع السـلوك الطبيعي الذي يعتمد على المسـتخدمين، أو المضيف، أو اتصال الشبكة، أو التطبيقات. على سـبيل المثال، قد يحدد وضع السـلوك الطبيعي لجهاز حاسب آلي مكتبي أن تصفح الإنترنت يتضمن (٢٠٪) في المتوسـط من اسـتخدام الشبكة خلال ساعات العمل العادية. وبعد ذلك تقوم (أنظمة كشف التسلل المُعتمدة على الانحرافات) بمقارنة النشاط الحالي ورفع الإنذار عندما يشـتمل نشـاط شـبكة الإنترنت على نطاق ترددي أكبر مما هو متوقع. وتشـمل الصفات الأخرى التي يمكن من خلالها إنشـاء أوضاع السـلوك الطبيعي على عدد رسـائل البريد الإلكتروني المرسـلة من قبل المسـتخدم، ومستوى استخدام المعالج للمضيف في فترة معينة من الزمن.

وتُعد (أنظمة كشـف التسـلل المُعتمدة على الانحرافات) أنظمة فعالة جداً في الكشف عن التهديدات التي لم تكن معروفة سابقاً. على سبيل المثال، في حالة إصابة جهاز الحاسب الآلي بنوع جديد من البرمجيات الخبيثة التي تُرسـل كميات كبيرة من البريد الإلكتروني غير المرغوب فيها، أو تسـتخدم موارد معالجة الحاسـب الآلي لكسر كلمات المرور، فإن سـلوك الحاسـب الآلي سيكون مختلفاً بشـكل كبير عن أوضاع السلوك الطبيعي التي أُنشئت لهذا الجهاز. وعندها سـتكون (أنظمة كشـف التسـلل المُعتمدة على الانحرافات) قادرة على الكشف عن هذه الانحرافات وتنبيه مسؤول النظام.

والمشـكلة الوحيدة في بناء أوضاع السـلوك الطبيعي لـ (أنظمة كشف التسلل المُعتمدة على الانحرافات) هي الصعوبة الكبيرة في تطوير أوضاع مرجعية ودقيقة للسلوك الطبيعي .

على سبيل المثال، قد يقوم جهاز الحاسب الآلي بعمليات نسخ احتياطي كاملة والتي تنطوي على كميات كبيرة من نقل البيانات الشبكية في اليوم الأخير من الشهر. وإذا لم يكن ذلك جزءاً من أوضاع السلوك الطبيعي، فإن صيانة مرور البيانات العادية سوف تُعد انحرافاً كبيراً عن أوضاع ذلك السلوك مما يؤدي إلى إطلاق الإنذارات.

أنظمة كشف التسلل المُعتمدة على حالات البروتوكول:

تقوم (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول) بمقارنة الأحداث المُلاحظة بنشاط البروتوكول المُحدد وذلك لكل حالة بروتوكول بهدف تحديد الانحرافات. وفي حين تَستخدم (أنظمة كشف التسلل المُعتمدة على الانحرافات) أوضاع سلوك طبيعي محددة للشبكة أو للمضيف، فإن تحليل حالات البروتوكول يُحدد كيف تُستخدم بروتوكولات معينة أو لا تُستخدم. على سبيل المثال، إن (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول) تعلم ما إذا كان المستخدم في حالة (غير مصادق) فإنه يجب أن يحاول عدد محدود من محاولات تسجيل الدخول، أو يجب أن يحاول فقط مجموعة من الأوامر الصغيرة في حالة (غير مصادق). إذاً فإن الانحرافات عن السلوك المتوقع للبروتوكول يمكن اكتشافها من خلال (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول). ومن القدرات الأخرى لـ (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول) هي القدرة على تحديد التسلسل غير المتوقع للأوامر. على سبيل المثال، إصدار الأمر نفسه مراراً وتكراراً يمكن أن يشير إلى هجوم القوة الغاشمة. كما تستطيع (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول) تتبع هوية المستخدم المستخدمة في كل جلسة وهو أمر مفيد عند التحقيق في حادث ما.

ويمكن أن يشمل تحليل البروتوكول فحص الأوامر الفردية مثل مراقبة أطوال المعامِلات. فإذا كان يحتوي الأمر عادة على معامِل (اسم المستخدم)، وكان طول هذا المعامِل ١٠٠٠ حرف فإن ذلك مثير للشك. وبالإضافة إلى ذلك، إذا كان اسم المستخدم يحتوي على بيانات غير نصية، فإن طول المعامِل السابق يُصبح أكثر غرابة ويستحق الإشارة إليه.

والعيب الأساسي في (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول) هو أن تتبع الحالة لجلسات عديدة في وقت واحد يستنزف الموارد الحاسوبية بشكل كبير مما يتطلب استثمارات كبيرة في المكونات المادية للحاسب الآلي.

هيكلة أنظمة كشف/ منع التسلل:

يتبع نشر (أنظمة كشــف/ منع التســلل) في المنظمة للهيكلة العادية للأنظمة الموزعة. وتحتوي المنظمة على العديد من عوامل الاستكشاف المنتشرة في جميع انحاء المنظمة والتي تقوم بجمع معلومات من الشبكة ومعلومات من المضيف. وتُرسل عوامل الاستكشاف تلك بياناتهــا إلى محطة الإدارة المركزية والتي تقوم بتســجيل جميــع البيانات الواردة في قاعدة بيانــات، كما تقوم بالتحليلات المختلفــة والمعتمدة على التوقيعــات والانحرافات وحالات البروتوكول. ويستخدم مســؤولو النظام وحدة تحكم مكتبية أو وحدة تحكم على الشبكة لتهيئة عوامل الاستكشاف، ومراقبة الإنذارات، واتخاذ الإجراءات الدفاعية المناسبة.

قيود أنظمة كشف/ منع التسلل:

تتضمن تكنولوجيا كشــف/ منع التسلل اثنين من القيود المعروفة: الإيجابيات الكاذبة والمراوغة.

مع الحالة الراهنة لهذه التكنولوجيا فإن أنظمة كشــف التســلل ليســت دقيقة تماماً. فالعديد من الإنذارات التي تُطلقها أنظمة كشــف التسلل لا تمثل تهديدات حقيقة، كما أن العديد من التهديدات الحقيقية تمر دون إطلاق إنذارات. وعملية الإشــارة إلى نشاط آمن بأنه نشــاط ضار تُدعى إيجابية كاذبة، أما الفشــل في تحديد النشــاط الضار فيُدعى سلبية كاذبة، والحد من إحدى هاتين العمليتين يؤدي عادة إلى زيادة العملية الأخرى. على سبيل المثال، نظام كشــف التسلل الحساس جداً سيكشــف هجمات أكثر واقعية، لكنه في الوقت نفســه سيُشــير إلى العديد من المعاملات الآمنة بأنها معاملات ضارة. ونظام كشف التسلل الأقل حساســية لن يُثير الكثير من الإنذارات الكاذبــة، لكن العديد من الهجمات الحقيقية قد تمر دون اكتشــافها. ولأن الهجمات الحقيقية مكلفــة جداً، فإن المنظمات تُفضل زيادة احتماليــة اكتشــاف حركة المرور الضــارة حتى لو كان ذلك يؤدي إلى الاســتجابة لكثير من الإنــذارات الكاذبة. ويأتي ذلك على حســاب فريق أمن المعلومــات حيث يتوجب عليهم تخصيص المزيد من الموارد للتدقيق في جميع الإنذارات الكاذبة للعثور على الأحداث الضارة بالفعل.

أما المراوغة فهي إجراء نشـاط ضار بحيث يبدو آمناً. ويسـتخدم المهاجمون إجراءات المراوغة للحد من احتمال اكتشـافهم من قبل تكنولوجيا أنظمة كشف التسلل. على سبيل المثال، يمكن أن يتم مسـح المنافذ ببطء شـديد (خلال عدة أيام) ومن عدة مصادر لتجنب الاكتشاف. كما يمكن إرسـال البرمجيات الضارة بوصفها أجزاء من مرفقات الملفات وتظهر بأنها آمنة.

ومن ثم فلا يمكن الوثوق بأنظمة كشـف/ منع التسلل لكشف جميع الأنشطة الضارة. ولكـن يمكن أن تكون تلك الأنظمة فعالة بوصفها جزءاً من النشر العام لأمن المعلومات في المنظمة كما هو الحال في الجُدُر النارية.

وتُعـد المبادئ التوجيهيـة الصادرة من المعهد الوطني للمعايـير والتكنولوجيا (NIST) مصدراً ممتازاً لمزيد من المعلومات حول تكنولوجيا أنظمة كشف/ منع التسلل.

إدارة تصحيحات أنظمة التشغيل والتطبيقات(٩):

التصحيـح هو برنامج يعمل على تصحيح المشـكلات الأمنيـة والوظيفية في البرمجيات والبرامج الثابتة. وتُسمى التصحيحات أيضاً بالتحديثات. وتُعد التصحيحات من أكثر الطرق فاعلية في الحد من آثار ثغرات البرمجيات. وفي حين يمكن للمنظمات أن تعالج مؤقتاً ثغرات البرمجيات من خلال الحلول المؤقتة (على سبيل المثال، وضع البرمجيات ذات الثغرات وراء الجُـدُر الناريـة)، تُعد التصحيحـات أو التحديثات من أكثر الطرق فاعليـة في التعامل مع ثغرات البرمجيات المعروفة.

أمـا إدارة التصحيحـات فهي عمليـة تحديد التصحيحـات والحصول عليهـا وتثبيتها والتحقـق منها. والتصحيحات مهمة بالنسـبة لمسـؤولي النظام وذلـك لفاعليتها في إزالة ثغـرات البرمجيات. وفي الواقع فـإن العديد من أُطر أمن المعلومات تفرض متطلبات إدارة التصحيحات. على سبيل المثال، يتطلب معيار أمن البيانات (Data Security Standard) التابع لصناعـة بطاقات الدفـع (Payment Card Industry) تثبيت التصحيحات المهمة خلال شهر واحد من إطلاق التصحيح (PCI DSS 2.0 متطلب رقم b.6.1).

---

(9) Souppaya, M. and Scarfone, K. Guide to enterprise patch management technologies (draft), NIST special publication 800-40 (accessed 11/24/2012)

وتواجه إدارة التصحيحات العديد من التحديات. وأهم تلك التحديات هو إمكانية كسر البرمجيات الحالية، خصوصاً تلك البرمجيات التي تم تطويرها داخلياً باستخدام التكنولوجيا القديمـة. وبحسـب معيـار أمـن البيانـات (Data Security Standard) التابع لصناعة بطاقات الدفـع (Payment Card Industry) فإن تصحيحات البرمجيات المناسـبة يمكن تعريفهـا بأنها «تلك التصحيحات التي تم تقييمها واختبارها بشـكل كاف لتحديد أن تلك التصحيحـات لا تتعارض مع التهيئة الأمنية القائمـة». وتتناول الإدارة الفاعلة للتصحيحات على مسـتوى المنظمة هذه التحديات وغيرها، وذلك حتى لا يقضي مسـؤولو النظم وقتاً في المشكلات التي يمكن الوقاية منها.

وفي السنوات الأخيرة اكتسبت برمجيات إدارة التصحيحات الآلية شعبية في التعامل مع هذه القضايا. وفي دراسـة مسـحية أجريت مؤخراً على أخصائيي تقنية المعلومات، أجاب (٦٤٪) من المشـاركين في الدراسة بأنهم يسـتخدمون منتجات برمجيات إدارة التصحيحات الآليـة مثـل (SUS, HFNetChk, BigFix Enterprise Suite, PatchLink Update) لإدارة التصحيحـات، و(١٨٪) يسـتخدمون تحديثات ويندوز، في حـين أن (١٧٪) ينفذون التصحيحات يدوياً[١٠].

وقـد حدد المعهد الوطني للمعايير والتكنولوجيـا (NIST) تحديات إدارة التصحيحات على مسـتوى المنظمة فيما يلي: التوقيت وتحديد الأولويات والاختبار، والتهيئة، والمضيف البديل، ومخزون البرمجيات، والموارد الزائدة الحمل، والتحقق من التطبيق. وسـنناقش كلاً منها باختصار في القسم التالي.

التوقيت وتحديد الأولويات والاختبار:

من الناحية المثالية، يجب تثبيت كل تصحيح بمجرد إصداره من قبل المورد وذلك لحماية الأنظمة في أسرع وقت ممكن. لكن إذا تم تثبيت التصحيحات دون إجراء اختبارات شـاملة سـيكون هناك خطر حقيقي لفشـل نظام التشـغيل مما يسـبب في تعطل فوري للمسـار الطبيعي للعمل في المنظمة. وعلى المدى القصير قد تنظر العديد من المنظمات إلى مثل تلك

(10) Gerace, T. and Cavusoglu, H. «The critical elements of the patch management process,» Communications of the ACM, 52(8), 2009: 117–121

الاضطرابات على أنها أكثر ضرراً من أي خطر محتمل من عدم تثبيت التصحيح. كما أن الأمور أصبحت أكثر تعقيداً من الناحية العملية لأن المنظمات غالباً ما يكون لديها نقص في الموظفين. وللحصول على أقصى قدر من المنافع من وقت الموظفين المحدود للتصحيحات، قد أصبح من الضروري أن تُحدد الأولويات بالنسـبة للتصحيحات التي يجب تثبيتها أولاً. لذلك فإنه أثناء إدارة التصحيح يكون التوقيت، وتحديد الأولويات، والاختبار في أكثر الأحيان في تعارض.

وأحد الحلول لهذا التحدي هو (حُزم التصحيح). فبدلاً من إصدار التصحيحات في أقرب وقت تكون فيه جاهزة، فإنه يتم إصدار مجاميع من تصحيحات عديدة كحزم تصحيح من قبل موردي المنتجات كل ربع سـنة أو بحسب جداول دورية. وهذا يقلل من جهد اختبار التصحيح في المنظمات، كما يسهل عملية النشر. ويمكن لحزم التصحيح القضاء على الحاجة لتحديـد الأولويـات إذا تم تقليل جهـود الاختبار والنشر بما فيه الكفايـة عن طريق حزم التصحيح. وحتى لو استخدم مورد البرمجيات حزم التصحيح فإنه سيقوم بإصدار التصحيح المناسـب على الفور بدلاً من الانتظار لوقت إصدار الحزمـة، وذلك إذا كان اختراق ثغرات البرمجيات غير المصححة معروفاً.

وفي أثناء تحديد أولويات التصحيحات من المهم النظر في أهمية الأنظمة التي سـيجري تصحيحها بالإضافة إلى أهمية الثغرات نفسها. فقد تكون الخوادم المواجهة لشبكة الإنترنت أكثر أهمية للتصحيح من أجهزة الحاسب المكتبية الموجودة في المنطقة المُسلحة. كما يجب النظر أيضاً إلى الاعتمادية. فإذا كان تثبيت تصحيح ما يعتمد على تثبيت تصحيحات أخرى أولاً، فـإن التصحيحـات المطلوبة أولاً سـتحتاج إلى اختبار وتطبيق حتـى إذا لم تكن ثغرة التصحيح في حد ذاتها مهمة جداً.

التهيئة:

في بيئـة المنظمات يُعد اختبار ونشر التصحيح معقداً بسـبب حقيقة وجود آليات عدة لتطبيق التصحيحات. على سبيل المثال، يمكن تهيئة بعض البرمجيات لتقوم بتحديث نفسها آلياً بواسطة المستخدم النهائي. وفي حالات أخرى، يقوم المستخدم بتثبيت بعض التصحيحات يدوياً أو يقوم بتثبيت أحدث إصدارات البرمجيات. وفي حين أن الأسلوب المفضل قد يكون

استخدام أداة مركزية لإدارة التصحيح فإنه في بعض الحالات قد يبدأ التصحيح بأدوات مثل ماسحات ثغرات الشبكات.

وقد تسـبب طُرق تثبيت التصحيحات المتنافسـة نوعاً من التعـارض. فقد تحاول تلك الطرق المتنافسـة الكتابة فوق التصحيحات، أو إزالة التصحيحات المُثبتة مُسـبقاً، أو تثبيت التصحيحـات التـي قررت المنظمة عدم تثبيتها لأسـباب الاسـتقرار التشـغيلية. لذا على المنظمات تحديـد جميع الطرق التي يتم تطبيق التصحيحات من خلالها، وحل أي تعارض بين طُرق تطبيق التصحيحات المتنافسة.

ويُعد المسـتخدم مصدر قلق ذا صلة بتهيئة إدارة التصحيحات. فالمستخدم، وخصوصاً المستخدم ذو السلطة، قد يتجاوز أو يتحايل على عمليات إدارة التصحيحات، مثلاً من خلال تفعيـل التحديثات المبـاشرة، أو تعطيل برمجيات إدارة التصحيحـات، أو تثبيت إصدارات قديمـة وغير معتمـدة من البرمجيات، أو إلغاء تثبيت التصحيحات. وإجراءات المسـتخدم تلـك تقوض من فاعلية عملية إدارة التصحيح. لذا عـلى المنظمات أن تتخذ خطوات لمنع المستخدم من التأثير سلباً في تقنيات إدارة التصحيح في المنظمة.

المضيف البديل:

تحتـوي بيئة المنظمة التقليدية على مجموعة واسـعة من المكونات المادية والبرمجيات المنتشرة في المنظمة. وتكون إدارة التصحيح مبسـطة بشكل كبير في الحالات التالية: تماثل جميع المضيفين، وفي حال إدارة المضيفين بشـكل كامل، وفي حال تشـغيل التطبيقات ونظم التشـغيل النموذجية. ويولد التنوع في البيئة الحاسـوبية تحديـات كبيرة خلال التصحيح. ومن أمثلة تنوع الهيكلة الحاسـوبية: المضيف المُدار بواسـطة المسـتخدم النهائي، وأجهزة الحاسـب الآلي المحمولة والمُسـتخدمَة في العمل عن بعد والتي تبقـى خارج بيئة المنظمة لفـترات طويلة والتي تعمل على جمع الثغرات، ومكونات تقنية المعلومات غير القياسـية مثل الثلاجات التي تدعم خدمة الإنترنت وغيرها من الأجهزة، والأجهزة المملوكة للأشخاص مثل الهواتف الذكية والتي لا تستطيع المنظمة السيطرة عليها، والافتراضية التي تعمل على إثارة وتدمير موارد أنظمة الحاسب الآلي، خصوصاً عند عمل الافتراضية ببرمجيات قديمة.

ومن القائمة أعلاه، تُعد الأجهزة حالة مثيرة للاهتمام بشكل خاص لأن الشركات المُصنعة لهذه الأجهزة ليسوا مُدركين غالباً لأهمية إدارة تصحيح الأخطاء، وقد لا تدعم تلك الشركات الإجراءات الآلية لاختبار ونشر التصحيحات. إن إدارة تصحيح الأخطاء لهذه الأجهزة يمكن أن تستهلك الكثير من الوقت، كما قد تتطلب عدداً كبيراً من الموظفين.

ويجب أن تنظر عملية إدارة التصحيح الفعالة بعناية إلى جميع هياكل المضيف البديلة والمرتبطة بالبنية التحتية لتقنية المعلومات في المنظمة.

مخزون البرمجيات:

للحصول على اختبـار فعّال، تتطلب إدارة تصحيح الأخطاء أن تحتفظ المنظمة بمخزون كامـل وحديث يتضمـن جميع البرمجيـات القابلة للتصحيح والمثبتة عـلى كل مضيف في المنظمـة. ويجب أن يحتوي هذا المخزون على الإصدار الصحيح، كما يجب أن يحتوي على حالة التصحيح لكل جزء من البرمجيات.

الموارد الزائدة الحمل:

بعـد اكتمال الاختبـار، تحتاج (عملية النشر) إلى الإدارة بطريقـة تمنع الموارد أن تصبح زائدة الحمولة. على سبيل المثال،

إذا بدأ العديد من المضيفين بتحميل تصحيح الأخطاء ذاته وفي الوقت نفسه، وكان ذلك التصحيح كبير الحجم، فإن ذلك سيؤدي إلى بطء كبير في سرعة التحميل لأن الأقراص الصلبة تبحـث عن الأجـزاء المختلفة للبرمجيات لكل مضيف على حدة. وفي المنظمات الكبيرة فإن عرض النطاق الترددي قد يصبح عائقاً ولاسـيما إذا كانت التصحيحات تُرسل عبر القارة من خلال شبكات الاتصال الواسعة (WAN). وعلى المنظمات أن تخطط لتجنب حالات زيادة حمولة الموارد. ولتحقيق ذلك فإن الإسـتراتيجية الشائعة هي تحجيم البنية التحتية لإدارة التصحيـح للتعامل مع كميات الطلب المتوقعة، والعمل على توصيل التصحيحات بشـكل متقطـع بحيث يقوم نظام إدارة التصحيح في المنظمـة بتوصيل التصحيحات لعدد محدود من المضيفين في أي وقت من الأوقات.

التحقق من التطبيق:

مسألة أخرى مهمة في إدارة تصحيح الأخطاء وهي إلزام المضيف المستهدف بالتغييرات المطلوبــة وذلــك حتى يأخذ التصحيــح أثره. واعتــماداً على التصحيــح والمكونات المادية والبرمجية المســتهدفة، فإن ذلك لا يحتاج إلى خطوة إضافية، بل قد يتطلب إعادة تشــغيل التطبيق أو الخدمة المُصححة، أو قد يتطلب إعادة تشــغيل نظام التشــغيل بأكمله، أو قد يتطلــب إجراء تغييرات أخــرى في حالة المضيف. وقد يكون مــن الصعب اختبار المضيف وتحديد ما إذا كان التصحيح قد أخذ أثره.

وإحدى آليات التعامل مع هذا التحدي هي استخدام وسائل أخرى لتأكيد التثبيت، مثلاً استخدام ماسح ثغرات مُستقل عن نظام إدارة التصحيح(١١).

حماية نقطة النهاية:

حماية (نقطة النهاية) هي عبارة عن الأمن المُطبق في جهاز المُســتخدم النهائي. وأجهزة المســتخدم النهائي هي أجهزة الحاسب المكتبية وأجهزة الحاسب المحمولة والأجهزة النقالة المســتخدمة مبــاشرة من قبل عملاء نظــام تقنية المعلومات. وعادة مــا يتم تنفيذ حماية (نقطة النهاية) باســتخدام تطبيقات برمجية متخصصة في تقديم الحماية مثل الحماية من الفيروســات، والحماية من البرامج الضارة، وكشــف التسلل. وتعمل حماية (نقطة النهاية) كخــط دفاع أخير في محاولة للتعامل مع المشــكلات الأمنية التــي لم تتعامل معها ضوابط الشبكة مثل الجُدُر النارية وأنظمة كشف التسلل.

وأمن (نقطة النهاية) يمكن أن يقدم أمناً لا تســتطيع أنظمة على مســتوى المنظمة أن تقدمه. على ســبيل المثال، تســتطيع أنظمة أمن (نقطة النهاية) تأكيد أن إصدارات نظام التشغيل، والمتصفح، وعميل البريد الإلكتروني، وغيرها من البرمجيات المُثبتة على الجهاز أنها مُحدثة، كما تقوم تلك الأنظمة بتنبيه المســتخدم لبــدء التحديث إذا لزم الأمر. والضوابط الأمنية القائمة على الشبكة لا يمكنها عادة توفير هذا المستوى الدقيق من الأمن.

---

(١١) وللاطلاع على لمحة عامة عن كيفية إدارة مايكروسوفت لتصحيحاتها الأمنية، انظر «Software vulnerability management at Microsoft,» at http://go.microsoft.com/?linkid=9760867 (accessed 07/22/2013)

وتعمــل حمايــة (نقطة النهاية) أيضاً على توفير حماية ضــد الأجهزة المخترقة داخلياً في الشبكة. على سبيل المثال، إذا كان هناك جهاز حاسب آلي مخترق داخل الشبكة، وقام هذا الجهاز المخترق بالبدء بمســح المنافذ داخل الشــبكة فإن برمجيــات حماية (نقطة النهاية) الموجودة على المضيف المســتهدف تستطيع كشف ذلك المسح، كما تستطيع منع الطلبات الأخرى من ذلك الجهاز حتى يتم حل هذه المسألة.

ومن الــشركات المعروفة في تقديم برمجيات حماية نقطــة النهاية شركة (Symantec) وشركة (McAfee). وتُقدم مايكروســوفت برنامج حماية يُدعى (Windows Defender) كجزء من نظام التشغيل.

العمليات:

تتعرف برمجيات أمن (نقطة النهاية) على البرمجيات الخبيثة والفيروســات باســتخدام إحــدى طريقتــين: توقيعات البرمجيات الخبيثة ومدى اشــتهارها. والكشــف القائم على التوقيعات هو الطريقة التقليدية في الكشــف عن البرمجيات الضارة. أما آليات الكشــف المُعتمدة على مدى اشــتهار البرمجيات الخبيثة فهي الأحدث، كما تُعد حاسوبياً أكثر كفاءة في الكشف عن التهديدات التي لم تكن معروفة مُسبقاً.

حماية نقطة النهاية المُعتمدة على التوقيعات:

لقد رأينا فيما ســبق أن التوقيع هو سلســلة من البايتات المعــروف عنها أنها جزء من البرامج الضارة. والتوقيعات هي التقنية السائدة المستخدمة في حماية (نقطة النهاية). وقد اعتمدت طرق الكشف عن الفيروسات والبرامج الضارة التقليدية على إجراء الخبراء لتحليل تفصيلي لكل فيروس وكل برنامج ضار قابل للتنفيذ، وذلك لتحديد سلســلة البايتات المُميزة للفيروس والبرنامج الخبيث. وبأســلوب التعبير الشــائع فإن سلسلة البايتات المحددة هي نفسها تعريف الفيروس. وبمجرد تحديد كل سلسلة بايتات، يتم إضافتها إلى قاعدة بيانات البرمجيات الخبيثة المعروفة التابعة لنقطة النهاية.

وتقــوم برمجيات حماية نقطة النهاية بفحص جميع الملفات الواردة والصادرة والمنفذة لمعرفة مدى وجود توقيع الفيروســات المعروفة. وإذا تم العثور على أحد تلك التوقيعات، يتم مباشرة حجر الملف.

ويواجه كشــف الفيروسات والبرامج الضارة اعتماداً على التوقيعات بعضاً من المشكلات المعروفة. والمشــكلة الأكثر وضوحاً هي عــدم إمكانية هذه الطرق الحماية من التهديدات غير المعروفة مســبقاً. فعندمــا يكون إصدار الفيروس حديثاً فــإن توقيع هذا الفيروس لن يكون موجوداً في قواعد بيانات (نقطة النهاية) ومن ثم فإن برمجيات حماية (نقطة النهاية) ستنظر إلى البرنامج على أنه برنامج آمن.

ثانياً، إن عدم قدرة (الكشــف المعتمد على التوقيع) على منع الفيروســات غير المعروفة تُشــجع نمو أعداد الفيروسات. نظرياً، يستطيع صانع الفيروس تعديل بايت واحد فقط من البرنامــج الضار ليُعيــق قدرة (الأنظمة المعتمدة على التوقيع) عــلى معرفة البرنامج الضار. وهذا يشــجع المطورين على إنشاء فيروسات تقوم بتعديل نفسها بمهارة عند الانتشار دون الحاجــة لأي تدخل مــن المطور مما يؤدي إلى تضخم في أحجام قواعــد بيانات التوقيعات. وبما أنه يجب فحص كل ملف ضد جميع التوقيعات المعروفة، فإن نمو حجم قاعدة بيانات التوقيعات يؤدي في نهاية المطاف إلى حقيقة أن (الكشف المعتمد على التوقيع) يسبب إبطاء النظام بشــكل ملحوظ. وقد أثر سباق التســلح هذا بين الفيروسات وتوقيعات الفيروسات سلباً على أداء النظام التابع لنقطة النهاية.

مدى انتشار توقيعات الفيروسات[١٢].

في عام ٢٠٠٨، اكتشفت شركة سيمانتك (Symantec)، وهي شركة متخصصة في حماية (نقط النهاية)، أكثر من ١٢٠ مليون برنامج ضار قابل للتنفيذ. وفي حين أن الشركة كانت في عام ٢٠٠٠ تنشر خمسة توقيعات لفيروسات جديدة كل يوم، فإن الشركة أصبحت تنشر في عام ٢٠٠٨ آلافاً من توقيعات الفيروسات الجديدة كل يوم. وهذه التوقيعات الجديدة كانت تُضاف بشكل مطرد إلى حِمل اكتشاف التوقيعات في كل جهاز، مما يؤدي إلى تعطل بعض الموارد الحاسوبية والتي يمكن استخدامها في مهام أكثر إنتاجية.

(12) http://www.symantec.com/connect/blogs/how-reputation-based-security-transforms-war-malware

حماية نقطة النهاية المُعتمدة على مدى اشتهار البرمجيات الخبيثة:

تحاول (حماية نقطة النهاية المُعتمدة على مدى اشتهار البرمجيات الخبيثة) تَنبؤ أمان الملف اعتماداً على نقاط الشهرة التي يتم حسابها بواسطة خواص الملف الملحوظة. ويتم حساب تأثير كل خاصية من خاصيات الملف على شــهرة الملف من الســلوك المُلاحظ للملفات على أجهزة المســتخدمين. ومع مرور الوقت يتم حساب نقاط الشهرة ويتم تحديثها دورياً لكل ملف معروف وقابل للتنفيذ[١٣]. وإذا تمت مواجهة برنامج حاسوبي قابل للتنفيذ فإن (نظام حماية نقطة النهاية المُعتمد على الشــهرة) يســتطيع تحديد أمــان ذلك البرنامج من خلال النظر في نقاط شهرته (إذا كانت معروفة) أو من خلال حساب شهرة البرنامج المُحتملة من خواص البرنامج الملحوظة.

وبما أن (حماية نقطة النهاية المُعتمدة على مدى اشتهار البرمجيات الخبيثة) تحتاج فقط إلى النظر في خواص الملف المعروفة (مثل حجم الملف، والعمر، والمصدر)، فإن هذه الطريقة تلغي الحاجة لمسح كل بايت في كل ملف بحثاً عن وجود أحد توقيعات البرمجيات الخبيثة المعروفة والتي يُقدر عددها بالملايين. وهذا يُسرِع من عملية مسح الفيروسات والبرمجيات الخبيثة بشــكل كبير مما يســمح بتكريس الموارد الحاســوبية إلى مهام أكثر إنتاجية مقارنة بطريقة كشف التوقيعات.

وتُعد الطرق المعتمدة على الشهرة مُصممة على مقاومة الفيروسات الجديدة. وتحصل الملفات غير المعروفة مسبقاً بشكل طبيعي على درجة شهرة منخفضة، ويشبه ذلك إلى حد كبير المُقترضين الجُدد مثل المراهقين الذين يبدؤون بدرجة ائتمان منخفضة. ومع استخدام الملف من قِبل أكثر من مستخدم ولفترات طويلة من الزمن ودون أي آثار ضارة، فإن درجة شــهرة الملف تتحســن. وهذا مشــابه لكيفية تحسين المســتخدم لدرجة ائتمانه من خلال تحمل مســؤولية القروض. لذا فإن الآليات المُعتمدة على الشــهرة تضع (علاوة) على مدى الإلمام بالملف ومن ثم فإنها تتمكن من إيقاف نمو متغيرات البرمجيات الخبيثة.

---

(١٣) تشير التقديرات إلى أن هناك أكثر من ١٠ مليارات ملف قابل للتنفيذ. المصدر: محادثة شخصية مع خبراء الصناعة في اجتماع مؤسسة العلوم الوطنية (NSF) الأول للباحثين الرئيسين حول إنترنت آمنة وموثوقة.

الأمن النسبي في مقابل الأمن المطلق

الغرض من الضوابط المُستعرضة في هذا الفصل هو الدفاع ضد معظم الهجمات والتهديدات العامة. على سبيل المثال، من تلك التهديدات المهاجم الذي يسعى لتثبيت الروبوتات (bots) على أي جهاز حاسب الآلي، بغض النظر عن ذلك الجهاز.

وعموماً يُعد الأمن نسبياً في هذه الحالات. فما دامت منظمتك أكثر أمناً من المنظمات الأخرى التي تعمل في ذات المجال، فإنك ستكون في مأمن لأن المهاجم سيركز على أسهل الأهداف. وهذا هو بالفعل النهج العام لأمن المعلومات.

وتشكل التهديدات المتطورة والمستمرة تحدياً جديداً. وتأتي التهديدات المتطورة والمستمرة على شكل هجمات مستهدفة يركز فيها المهاجمون على منظمة معينة لأي سبب من الأسباب (عادة لاختراق الملكية الفكرية). وسوف يحاول المهاجمون بكل ما لديهم من وسائل للحصول على ما يريدون. وفي هذه الحالة يعد الأمن أمناً مطلقاً. وما تحتاج إليه المنظمة عملياً أن تكون آمنة بحيث لا يمكن اختراقها بواسطة المحاولات المستهدفة من قبل المهاجم.

نموذج حالة - شبكات شركة (AirTight):

في عـام ١٩٩٥ أكمل برافـين باغوات (Pravin Bhagwat) الدكتوراه في الحاسـب الآلي مـن جامعة ماريلاند (University of Maryland) في كلية (College Park). وبعد ذلك عمل باحثاً رئيسياً في مركز بحوث (AT&T Research and IBM Thomas J. Watson). وبحلول عام ٢٠٠٣ أصبح برافين باحثاً معروفاً في مجال الشـبكات اللاسـلكية حيث شـارك في تأليف ٥ براءات اختراع في جوانب مختلفة من الشـبكات اللاسـلكية(١٤). وفي المحاولات المبكرة التي تمت في تلك الأيام، كانت الصناعة تسـعى لإيجاد إصدار لاسـلكي من شـبكة الإيثرنت (Ethernet). وكان الهدف تمكين أجهزة الحاسـب الآلي من إرسـال البيانات دون الحاجة إلى أسـلاك لنقل البيانات. وبدأ التسـويق لهذه التقنية في عام ١٩٩٧ عندما قامت جمعية مهندسي الكهرباء والإلكترونيات (IEEE) بنشر معيار (٨٠٢,١١) لتكنولوجيا إيثرنت اللاسـلكية الناشـئة. وحدد هذا المعيار معدل نقل البيانات ليصل إلى ٢ ميجابت في الثانية وكان مصمماً في الأسـاس للاسـتخدام من قبل الماسـحات الضوئية في متاجر البيع بالتجزئة

(14) http://patft.uspto.gov/netahtml/PTO/search-adv.htm

والمستودعات. وفي عام ١٩٩٩ تم نشر معيار (٨٠٢,١١b) والذي يحدد معدل نقل البيانات ليصــل إلى ١١ ميجابــت في الثانية. وعندمــا أدركت الشركات المصنعة للحاســب الآلي أن معدلات نقل البيانات تلك قابلــة للمقارنة بمعدلات نقل الإيثرنت للبيانات والتي تصل إلى ١٠ ميجابايــت في الثانية، رأت الشركات المُصنعة أنــه بالإمكان إضافة هذه التقنية بوصفها جزءاً متكاملاً من اللوحة الأم لأجهزة الحاسب الآلي.

إن تكامل شــبكات الواي فاي (wi-fi) في أجهزة الحاســب الآلي أعطى إشارة إلى برافين أن الشــبكات اللاسلكية ستُصبح قريباً التكنولوجيا السائدة. كان يرى أنه قريباً سيُصبح من المألوف للمســتخدمين حمل أجهزة الحاســب الآلي في حقائب اليد (أجهزة الحاســب الآلي المحمولة). وبعد أن أمضى سنوات عديدة في هذا المجال بصفة متخصص، بدأ التفكير جدياً في اقتناص الفرص الريادية في هذا القطاع.

والخيار الواضح كان الدخول في مجال أعمال تقديم نقاط الوصول اللاســلكية. لكن في الوقت الذي حدد فيه برافــين الفرصة، كانت هناك شركات مثل (Aruba) و(Airespace) و(Trapeze) و(Vivato) و(Airgo) و(Aerohive) قــد حصلــت بالفعل على مســتويات تمويل عالية من العديد من المستثمرين. والمنافسة في هذا المجال تعني التنافس مع شركات ممولــة تمويلاً جيداً مع إمكانية وصولهم إلى أفضل المستشــارين في الصناعة. وللدخول في هــذا المجــال، وضع برافين نموذجاً من ثلاث خطوات كما يلي: (١) توقع مشــكلة ما، و(٢) صمــم «مصيدة» رائعة لحل تلك المشــكلة، و(٣) كن جاهزاً لخدمــة العملاء عندما تظهر المشــكلة المتوقعة. ومع العلم أن الآخرين قد تغلبوا عليه في هذه الفرصة، إلا أنه قرر أن يتطلــع إلى الأمام لمعرفة الفرص القادمة في هذا القطاع. وليس ذلك فحســب فقد قرر أن يكون مستعداً بالحلول عندما يتوصل إلى تلك الفرص.

الثغرات باعتبارها فرصة عمل:

الخبرة المكتســبة من اقتحام تطــور التكنولوجيا في مهدها أعطــت برافين بعض الرؤى الفريدة من نوعها. لقد أدرك أن إدخال الشبكات اللاسلكية سوف يكشف عن فئة جديدة وكاملة من الثغرات داخل المنظمات. وبالتحديد فإن الأعمال التجارية إلى الآن لا تُعد أسلاك

شـبكة الإيثرنت (طبقة ٢) مصدراً للتهديدات. وأسلاك شبكة الإيثرنت تكون عادة معزولة داخل المباني حيث يتطلب الدخول إليها بعضاً من الإجراءات الأمنية المادية التقليدية التي تحول دون وصول المهاجمين لتلك الأسلاك مما يحول دون إحداث الأضرار. لذا فإن معظم الثغـرات الأمنية في هذه البيئة تحدث في طبقة الشـبكة أو الطبقـات الأعلى. وبما أن كل حركة المرور عبر المنظمات تمر من خلال موقع مركزي، وهو بوابة الموجه الشبكي، فإن جداراً نارياً بقواعد واضحة المعالم يكون كافياً للتعامل مع معظم الهجمات في معظم المنظمات.

ولكن ذلك سـيتغير إذا تـم إيصال نقاط وصـول الواي فاي مباشرة بشـبكة الإيثرنت. فالإشارات اللاسلكية تنتشر في جميع الاتجاهات. وفي المجمع الكبير الذي يضم العديد من المكاتب، فإن الإشارات اللاسلكية من شركة ما يمكن رصدها من الشركة المجاورة. وسيصبح مـن الممكن فحص الحزم وتعديلها وحقنها في الشـبكة بشـكل غير مـصرح به من خارج الشبكة من خلال نقاط الوصول تلك، أو من خلال مجرد الوقوف في البهو. وكانت تلك ثغرة جديدة تماماً ومن شأنها أن تؤثر حتماً في كل منظمة في العالم.

ولأن برافين يُدرك أنه لا أحد يعلم عن الفرص التجارية لهذه الثغرة، قرر العمل نحو إيجاد حل لهذه المشـكلة. وبدأ بوضع مـا أعده برافين العناصر الثلاثة الأساسـية لبداية المشروع: فكرة، وفريق عمل، والموارد المالية اللازمة لدعم الفريق حتى يتم الوصول إلى الأرباح.

لكـن مـا المصيدة الرائعة في أمن المعلومات؟ هل هي نظـام منع الاختراق؟ لكن هذا النظـام يُعد تكنولوجيا معروفة. هل المصيدة الرائعة أمر يُخفض التكلفة؟ كيف يمكنك أن تفعل ذلك؟ ربما من خلال أتمتة شيء ما؟ وبعد الكثير من التفكير خُلص إلى أن شيئاً يقوم بأتمتة وظائف إدارة النظام الأساسية قد يكون مفيداً.

وبناء على ذلك ركزت الشركة على أتمتة الكشف عن نقاط الوصول الضارة، وأتمتة مسح الشـبكة اللاسـلكية. وبحلول نهاية عام ٢٠٠٥، أي بعد عامين من التطوير المُكثف، أصبح لـدى برافين الحل العملي لهذه المشـكلة. وفي حين أن الحلـول القائمة تحدد جميع نقاط الوصول المتاحة على الشـبكة (الشـكل ٩-٦)، فإن الحل الذي طوره برافين يحدد كل نقطة وصـول في المنطقة المحيطـة كنقطة داخلية، أو نقطة خارجية، أو نقطة خطيرة، أو نقطة لم يتم تهيئتها بالشكل الصحيح (الشكل ٩-٧). وهذه التقنية تسمح لمسؤول الشبكة بتحديد نقاط الوصول التي تحتاج إلى انتباه بكل وضوح (تلك باللون الأحمر في الشكل ٩-٧).

الشكل (٩-٦): لوحة تحكم تقليدية لأحد المنافسين (circa 2003)

MAC	SSID	Enc...
000FCC5AE59C	BPMVR	WEP
001C106C6928	zguest	
0019A9A7C131	gear6-guest	
0030AB1EF491	nothere	WEP
001C106C63D8	zguest	
00237521D0C0	1037 1665	WEP
000FCCFEE1C0	7756 7014	WEP
001195E0F2D8	matissenetg	WPA2
001E5823BF27	matisseguest	WEP
00121762B57D	linksys-g	
000D0B2B0C1B	spectra	WEP

الشكل (٩-٧): لوحة تحكم تابعة لشركة (circa 2005) AirTight

	RSSI	Name	MAC Address	Channel	Protocol	No. of ...	SSID	Security
		AirTight_A0:82:00	MULTIPLE	MULTI...	a/b/g [...	0	MULTIPLE	802.11i
		AirTight_A0:B2:00	00:11:74:A0:8...	36	a [802....	0	anw	802.11i
		AirTight_A0:B2:00	00:11:74:A0:8...	1	b/g [80...	0	@NAT	802.11i
		AirTight_01:00:11	MULTIPLE	52	a [802.1...	20	MULTIPLE	Open
		AirTight_01:00:21	MULTIPLE	6	b/g [80...	20	MULTIPLE	Open
		00:CF:5F:33:C4:21	00:CF:5F:33:C...	10	b/g	14	cream_hotspot	Open
		Cisco-Linksys_06:8...	00:16:B6:06:8...	14	b	0	Test_212	802.11i
		Cisco-Linksys_10:B...	C0:C1:C0:10:8...	1	b/g	0	choochee-cell	802.11i
		AirTight_A0:48:50	00:11:74:A0:4...	11	b/g [80...	0	AA_BGN_1	802.11i
		D-Link_7F:7A:62	14:D6:4D:7...	6	b/g [80...	0	dlink-bgn	802.11i, ...

والعنصر الأساسي في تكنولوجيا شركة (Airtight) هو صندوق مادي يضاف إلى الشبكة. ويقوم هذا الصندوق باستشــعار الإشــارات اللاســلكية في المحيط ليجمــع كل المعلومات المطلوبة، كما يقوم بمعالجة الإشارات باستخدام الخوارزميات التي تملكها الشركة.

محفز السوق:

وفي حــين أن التكنولوجيــا مثيرة للاهتمام ومقنعــة، إلا أن برافين سرعان ما واجه حاجزاً آخر. فعندما بدأ برافين بتســويق التكنولوجيا لاحــظ أن العملاء المُرتقبين لم يدركوا أهمية اتخــاذ أي إجراء عاجل. وبالنتيجة فإن برافين كان يحــاول إقناع العملاء بإنفاق المال لحل مشــكلة محتملة غير موجودة ســابقاً ولم يتعــرض لها أحد منهم أبــداً. وكأنه كان يحاول بيع الأســبرين لأشــخاص لم يعانوا من الصداع أبداً. وفي عام ٢٠٠٥، لم تكن الحلول الأمنية للشــبكات اللاســلكية شرطــاً مفروضاً على الشركات من قبل مســؤولي الولايــة أو الهيئات الصناعية مثل اتحــاد صناعة بطاقات الدفع (Payment Card Industry). ولا أحد يريد أن ينفق المال على أمن المعلومات إلا إذا توجب عليهم فعل ذلك. وأي شخص مهتم بأمن الشــبكات اللاســلكية فإنه سيكون ســعيداً بأي مســتوى من الأمن يقدمه المورد مع نقاط الوصول المُصممة في النظام.

والطريقــة التــي عملت بها الشركة اعتبــاراً من عام ٢٠٠٧ أن النجــاح كان محدوداً في الصناعات التي يكون للأمن فيها أولوية عالية مثل المؤسســات المالية، وشركات الاتصالات، والقطــاع الحكومي. وقــد أدرك مديرو تقنية المعلومات في هــذه المنظمات ذلك التهديد، وكانوا على اســتعداد للاســتثمار في الحلول التقنيــة التي تُضيف طبقــة إضافية من الأمن لشبكاتها اللاسلكية الحالية.

وخلال الأعوام من ٢٠٠٣ إلى ٢٠٠٧، استمرت الشركة في العمل من خلال ما يعده برافين الأساسيات الثلاثة للمحافظة على الشركة بعد انطلاقها: الجهد، والوقت والصبر، ورأس المال. وحصــل برافين على التمويل من الشركات الاســتثمارية التي اقتنعــت برؤية برافين، وهي شركات ذات سمعة طيبة ومن جميع أنحاء العالم.

لكن كل هذا تغير عندما أصبح ألبيرتو جونزاليس (Alberto Gonzalez) وأنشــطته في شركــة تي جي ماكس (TJ Maxx) معروفة. فقــد أصبحت الشركات مُدركة للخطر الجديد الذي أنشــأته الشبكات اللاسلكية. وبالإضافة إلى ذلك فإن إصدار رقم (١,١) لمعايير (PCI) قــد طرح مُتطلباً لجميع الــشركات التي تقبل البطاقات الائتمانية بضرورة المســح الدوري للشــبكات اللاسلكية لتحديد نقاط الوصول غير المهيأة بشكل جيد (لم يكن هناك مثل هذا

المتطلب قبل وقوع حادثة تي جي ماكس). وهكذا ساعد ألبرتو جونزاليس بتوعية زبائنه بطريقة لم يتمكن هو من مساعدة نفسه بها. وفجأة أصبحت الشركات تعاني من الصداع وأصبحت تبحث عن الأسبرين الذي يمكن أن توفره شركة (AirTight).

الوضع الحالي:

تلقت شركة (Airtight) العديد من جوائز الصناعة على مر السنين. وفي وقت كتابة هذا الكتاب، كان لدى الشركة ٢٩ براءة اختراع تغطي جوانب مختلفة من التكنولوجيا التي طورتها الشركة. وفي عام ٢٠١٢ وضعت شركة (Gartner MarketScope)، وهي شركة لأنظمة منع اختراق شبكات الاتصال اللاسلكية المحلية، مُنتج (Airtight Networks) تحت تصنيف (إيجابي قوي) حيث تُعد شركة (Airtight) الشركة الوحيدة التي حققت هذا التصنيف في حقل يضم منتجات من قادة الصناعة مثل شركة (Cisco) وشركة (Motorola) وشركة (Aruba Networks). وقد عززت ميزات هذا المنتج تحقيق مزيد من النجاح مما أدى إلى جذب مجموعة من العملاء مثل شركة (Citrix) وشركة (New York City Transit) وشركة (Ryder Systems).

الاتجاهات المُستقبلية:

وبعد سيطرة شركة (Airtight) على سوق أمن شبكات الواي فاي لعدة سنوات، تتطلع الشركة الآن للتوسع عن طريق الدخول إلى أسواق أكبر. هل تذكر سوق الوصول اللاسلكي الذي يئس برافين من الوصول إليه في الأيام الأولى للشركة لكونه متأخراً في دخول ذلك السوق؟ الآن تبحث شركة (AirTight) دخول هذا السوق بالتحديد، وذلك بعد إقامة علاقات مع بعض كبار العملاء من خلال تقديم عروض أمن الشبكات اللاسلكية لها. ومن المتوقع أن ترتفع إيرادات سوق الوصول اللاسلكي من ٤ مليار دولار تقريباً في عام ٢٠١٣ إلى نحو ٢٠ مليار دولار في عام ٢٠٢٠. وتعتقد شركة (AirTight) أنه ما دام بإمكانها تحقيق الأمن بالشكل الصحيح، على الرغم من أن المعروف عن تقنيات الأمن على نحو واسع بأنها تقنية صعبة الإتقان، فإنه سيكون بإمكان الشركة أيضاً تحقيق الوصول بالشكل الصحيح.

وتقــوم شركــة (AirTight) بجهود في العديد من الصناعات التي فيها انتشــار واســع للشــبكات اللاســلكية الموزعة مثل تجارة التجزئة، والضيافة، والرعايــة الصحية، والتعليم. والــشركات في هذه الصناعات كبيرة لكن احتياجاتها الأمنيــة متواضعة. وقد دخلت شركة (AirTight) هــذه الصناعات من خلال تقديم الميزات التي قد تكون ذات فائدة لكل من هذه القطاعات. على ســبيل المثال، يستطيع العملاء تفعيل قدرات الوصول إلى شبكة واي فاي باســتخدام الأجهزة الأمنية المنتشرة مع ترقية بســيطة للبرمجيات. وفي قطاع التعليم العالي، تقوم شركة (AirTight) بتطوير الميزات التي تســمح للأســاتذة والطلاب بدراســة شــبكات الحاسوب عن طريق اختبار شــبكات المرور التي تم تصفيتها مباشرة داخل الحرم الجامعي.

وفي وقــت كتابة هذا الكتاب، أي في منتصف عام ٢٠١٣، حققت شــبكات (AirTight) انتصارات رئيســية لوصول شــبكات الواي فاي في قطاع التجزئــة. وقد انتشرت تكنولوجيا شركة (AirTight) في آلاف المواقع لبعض محلات التجزئة المحلية المشــهورة. وأحد الميزات المنتــشرة في محلات بيع التجزئة هــي الخدمات التحليلية للبيانــات الضخمة التي تهدف لمساعدة هذه الشركات في تتبع الزوار وتقديم عروض ترويجية مخصصة من خلال الهواتف المحمولة. وتسمح ميزة أخرى لهذه المنظمات بتقديم وصول آمن للشبكة اللاسلكية في كل موقع، وذلك بتحقيق الحد الأدنى من التهيئة لكل محل.

ولمعالجة محدودية الميزانيات المالية في التعليم العالي، طورت شركة (AirTight) حلول نقاط الوصول اللاسلكية والمدارة بالحوسبة السحابية، وذلك للقضاء على أحد أغلى مكونات النــشر التقليدي للشــبكات المحلية في الحرم الجامعي. وهذا النموذج يســمح ببســاطة للمنظمات بنشر نقاط الوصول اللاســلكية على الشــبكة حيث تقوم بتهيئة نفسها تلقائياً. ويقوم مسؤولو الشبكة بإدارة نقاط الوصول باستخدام واجهة بسيطة لمتصفح الشبكة.

وقــد أطلقت شركــة (AirTight) على تلك المنتجات (نقاط الوصول اللاســلكية الذكية والمدارة بالحوسبة السحابية) مقارنة بـ (نقاط الوصول التقليدية والخفيفة والمُدارة بوحدة تحكم). وهذه التغييرات الهيكلية رفعت من مدى تطوير المكونات المادية للحاســب الآلي على مدى العقد الماضي. وبما أن وحدات المعالجة المركزية أصبحت أسرع، وذاكرات الوصول

العشـــوائي أصبحت أرخص، وأصبحت المعايير سائدة، فإن المقايضات التي أوجبت استخدام وحدات التحكم المركزية قد تغيرت. والآن بإمكان نقاط الوصول غير المكلفة أن تحل محل التكنولوجيا التي كانت باهظة التكاليف قبل عقد واحد فقط. إن صناعة الوصول اللاسلكي والتي مرت خلال مرحلتين من التغييرات الفوضوية(١٥) قد تكون معرضة لتغيير فوضوي آخر في حياتها التي ما زالت قصيرة.

المراجع:

Wireless Field Day 5 presentation by David King, CEO of AirTight Networks, http://www.youtube.com/watch?v=qxNAUeevfvc&list=PLObjX_zORJMAz0EBXmsQqSS5EOWzb96St&index=16 (accessed 813/11/)

محادثة شخصية مع بطل الحالة بواسطة أحد مؤلفي هذا الكتاب

أسئلة مراجعة للفصل:

١. ما مفهوم كلمات المرور؟ وفيمَ تُستخدم؟

٢. اشرح باختصار بعض الأشكال البديلة لكلمات المرور.

٣. ما إدارة كلمات المرور؟ وما أهميتها؟

٤. ما التهديدات المهمة لكلمات المرور؟

٥. ما التوصيات المهمة لإدارة كلمات المرور؟

٦. ما هي بعض إيجابيات وسلبيات كلمات المرور؟

٧. ما الجُدُر النارية؟ وما استخداماتها العامة؟

٨. اكتب مثالاً لقاعدة جدار ناري باســتخدام الصياغة الموضحة في هذا الفصل. اشرح ما تقوم به هذه القاعدة.

(١٥) المرحلة التي كان فيها مرور الشبكة يُدار بواسطة نقاط الوصول كانت تُعد المرحلة الأولى، في حين يُعد استخدام وحدات تحكم مركزية لإدارة مرور الشبكة المرحلة الثانية.

٩. اكتب قاعدة لجدار ناري تقوم بحظر جميع الطلبات الواردة (منفذ ٨٠) من شبكة (١٦/١٩٢,١٦٨,٠,٠).

١٠. ما هي بعض قيود الجُدُر النارية؟

١١. ما الجُدُر النارية للفحص العميق للحُزم؟ وما الإمكانات الإضافية التي توفرها مقارنة بالجُدُر النارية لتصفية الحُزم؟

١٢. ما الفروق بين الشبكة المحيطة والشبكة الداخلية من وجهة نظر أمن المعلومات؟

١٣. ارسم مخططاً لجدار ناري تقليدي في منظمة ما موضحاً الجدار الناري المحيط، والجدار الناري الداخلي، والمنطقة المنزوعة السلاح، والشبكة الداخلية.

١٤. ما التوصيات الأساسية لتهيئة الجدار الناري؟

١٥. ما أنظمة كشف/ منع التسلل؟

١٦. ما (أنظمة كشف التسلل المُعتمدة على التوقيعات)؟ وما إيجابياتها وما عيوبها؟

١٧. ما (أنظمة كشف التسلل المُعتمدة على الانحرافات)؟ وما إيجابياتها وما عيوبها؟

١٨. ما (أنظمة كشف التسلل المُعتمدة على حالات البروتوكول)؟ وما إيجابياتها وما عيوبها؟

١٩. ما التصحيح؟ وما حزم التصحيح؟ ولماذا تُستخدم؟

٢٠. ما إدارة التصحيح؟

٢١. اشرح باختصار أهم التحديات التي تواجه إدارة التصحيح الفعالة.

٢٢. ما حماية نقطة النهاية؟ وهل هي ضرورية في المنظمات التي تحتوي على ضوابط شبكة قوية مثل الجُدر النارية وأنظمة كشف التسلل وكلمات المرور القوية؟

٢٣. ما هي بعض الخدمات الهامة التي توفرها حماية نقطة النهاية؟

٢٤. ما هي بعض القيود في الحماية من البرامج الضارة المعتمدة على التوقيعات؟

٢٥. ما الحماية من البرامج الضارة المُعتمدة على الشهرة؟

أسئلة على نموذج الحالة:

١. قدم مُلخصاً للمتطلبات الأمنية للشــبكات اللاسلكية (سيُرشدك البحث في الإنترنت عن مصطلح «PCI wireless requirements» إلى بعض المصادر المفيدة)

٢. افترض أنك (مدير معلومات) في منظمة متوسطة إلى كبيرة الحجم. ما مدى أهمية حجم الشركة الموردة في قرارك لاســتخدام منتجاتهــا في أمن معلومات منظمتك؟ ولماذا حجم الشركة الموردة يُمثل أهمية بالنسبة لك؟

٣. افترض أنك (مدير معلومات) في منظمة متوسطة إلى كبيرة الحجم. ما مدى تأثير الوجود المُســبق لتكنولوجيا المورد في منظمتك على قرارك لاســتخدام منتجاته في أمن معلومات منظمتك؟ ولماذا تمثل الخبرة السابقة مع المورد أهمية بالنسبة لك؟

٤. افترض أنك (المدير التنفيذي) لمنظمة ناشــئة تُقدم منتجات مؤثرة في تحسين أمن معلومات المنظمة. كيفك يمكنك معالجة القضايا التي أُثيرت في السؤالين السابقين؟

٥. قم بزيارة الموقع الإلكتروني لشركة (AirTight). ما المنتجات والخدمات الأساسية التي تقدمها الشركة؟

نشاط التدريب العملي - نظام كشف التسلل المعتمد على المضيف (OSSEC):

في هذا التمرين ســوف نعمل على نظام (OSSEC)، وهو نظام كشــف تســلل معتمد عــلى المضيف ومفتوح المصدر، حيث ســنقوم بتثبت واختبار هــذا النظام على آلة لينكس الافتراضية التي ســبق الحديث عنها في الفصول الســابقة. ويقوم نظام (OSSEC) بتحليل الســجل، والتحقق من تكامل الملف، ومراقبة السياســات، والكشــف عن الجذور الخفية، والتنبيه في الوقت الفعلي، والاستجابة الفعالة. ولمزيد من المعلومات راجع الموقع الإلكتروني لنظام (OSSEC) (http://www.ossec.net).

ولتثبيت نظام (OSSEC)، افتح نافذة طرفية واستخدم (su) لحساب الجذر:

```
alice@sunshine ~]$ su -
Password:  thisisasecret
```

انسخ ملفات تثبيت نظام (OSSEC) إلى دليل مؤقت، وفك ضغط الملف وابدأ عملية التثبيت.

```
[alice@sunshine  ~]#  cp  /opt/book/con-
trols/packages/ossec-hids-2.7.tar.gz   /
tmp/.
[alice@sunshine ~]# cd /tmp
[alice@sunshine  /tmp]# tar zxvf ossec-
hids-2.7.tar.gz
[alice@sunshine /tmp]# cd ossec-hids-2.7
[alice@sunshine /tmp/ossec-hids-2.7 ]# ./
install.sh
```

```
** Para instalação em português, escolha [br].
** 要使用中文进行安装，请选择[cn].
** Fur eine deutsche Installation wohlen Sie [de].
** εια εγκατάστασηστα Eλληνικά, επιλεξτε [el].
** For installation in English, choose [en].
** Para instalar en Español, eliga [es].
** Pour une installation en français, choisissez [fr]
** A Magyar nyelvü telepítéshez válassza [hu].
** Per l'installazione in Italiano, sce- gli [it].
** 日本語でインストールします．選択して下さい[jp].
** Voor installatie in het Nederlands, kies [nl].
** Aby instalować w jezyku Polskim, wybi- erz [pl].
** Для инструкций по установке на русском, введите[ru].
** Za instalaciju na srpskom, izaberi [sr].
** Türkçekurulum için seçin [tr].  (en/br/cn/de/el/es/fr/hu/it/jp/nl/pl/ru/
sr/tr) [en]:  en
```

```
OSSEC  HIDS  v2.7 Installation Script -
http://www.ossec.net
You are about to start the installation
process of the OSSEC HIDS.
You must have a C compiler pre-installed
in your system.
If you have any questions or comments,
please send an e-mail to dcid@ossec.net
(or daniel.cid@gmail.com).
-  System:   Linux  sunshine.edu  2.6.32-
279.2.1.el6.i686
- User:  root
- Host:  sunshine.edu
-- Press ENTER to continue or Ctrl-C to
abort.  --
1- What kind of installation do you want
(server, agent, local, hybrid or help)?
local
- Local installation chosen.
2- Setting up the installation environment.
- Choose where to install the OSSEC HIDS
  [/var/ossec]:  /var/ossec
- Installation will be made at /var/
  ossec.
3- Configuring the OSSEC HIDS.
3.1- Do you want e-mail notification?
     (y/n) [y]:  y
  - What's your e-mail address? root@
    localhost
  - We found your SMTP server as:  127.0.0.1
  - Do you want to use it? (y/n) [y]:  y
--- Using SMTP server:  127.0.0.1
3.2- Do you want to run the integrity
     check daemon? (y/n) [y]:  y
  - Running syscheck (integrity check
    daemon).
3.3- Do you want to run the rootkit detec-
     tion engine? (y/n) [y]:  y
  - Running rootcheck (rootkit detection).
3.4- Active response allows you to exe-
     cute a specific
     command based on the events received.
     For example,
     you can block an IP address or dis-
     able access for
     a specific user.
     More information at:
     http://www.ossec.net/en/manual.
     html#active-response
```

```
 - Do you want to enable active response?
   (y/n) [y]:  n
  - Active response disabled.
3.6- Setting the configuration to analyze
     the following logs:
-- /var/log/messages
-- /var/log/secure
-- /var/log/maillog
-- /var/log/httpd/error_log (apache log)
-- /var/log/httpd/access_log (apache log)
- If you want to monitor any other file,
  just change
  the ossec.conf and add a new localfile
  entry.
  Any questions about the configuration
  can be answered
  by visiting us online at http://www.
  ossec.net.
--- Press ENTER to continue ---
- System is Redhat Linux.
- Init script modified to start OSSEC
  HIDS during boot.
- Configuration finished properly.
- To start OSSEC HIDS:
       /var/ossec/bin/ossec-control start
- To stop OSSEC HIDS:
       /var/ossec/bin/ossec-control stop
- The configuration can be viewed or mod-
  ified at /var/ossec/etc/ossec.conf
  Thanks for using the OSSEC HIDS.
  If you have any question, suggestion or
  if you find any bug,
  contact us at contact@ossec.net or using
  our public maillist at
  ossec-list@ossec.net
( http://www.ossec.net/main/support/ ).
  More information can be found at http://
  www.ossec.net
--- Press ENTER to finish (maybe more
information below).  ---
```

يمكنك الآن تشغيل نظام (OSSEC) باستخدام الأمر الموضح أعلاه، لكن قبل ذلك يجب تعديــل أحد خيارات التهيئة حيث يتم افتراضياً تشــغيل فحص نظــام (OSSEC) كل ٢٢ ســاعة. وهذا لا بأس به للاســتخدام العادي. لكن سنحتاج إلى تشغيل هذه العمليات أكثر من ذلك في هذه التمارين. ستحتاج إلى فتح الدليل التالي في محرر نصي (//var /ossec/ etc ossec. conf) ومن ثم تغيير القيمة في ســطر ٧٦ من ٧٩٢٠٠ (تحويل ٢٢ ســاعة إلى ثوان) إلى ٣٠٠ وبعــد ذلك تقوم بحفظ التغييرات. لاحــظ أن ملف (ossec. conf) يمكن عرضه وتعديله فقط بواســطة الجذر. وعند تسجيل دخولك كجذر، قم بتعديل الملف باستخدام المحرر النصي (Gnome Text Editor) (شكل ٩-٨).

```
alice@sunshine etc]# gedit /var/ossec/
etc/ossec.conf
```

ولتفعيل أرقام السطور في المحرر النصي (Gnome)، اختر ملف (File) ← خيارات (Preferences)، وقم بتمكين خانة الاختيار لـ «عرض أرقام السطور» (Display line numbers)

```
<!-- Frequency that syscheck is executed
- default to every 22 hours →
<frequency>300</frequency>
```

وســيؤدي هذا التعديل إلى تشــغيل فحص نظــام (OSSEC) كل ٥ دقائق بدلاً من ٢٢ ساعة. وبعد القيام بهذا التعديل يمكنك الآن تشغيل خادم (OSSEC). قم بحفظ التغييرات ومن ثم إنهاء المحرر النصي (Gnome)، ثم ارجع إلى موجه النافذة الطرفية.

الشكل (٩-٨): دليل (var /ossec/ etc/ ossec. conf/) (بعد التعديل)

```
*ossec.conf (/var/ossec/etc) - gedit
File Edit View Search Tools Documents Help
Open  Save  Undo
*ossec.conf
65      <include>ossec_rules.xml</include>
66      <include>attack_rules.xml</include>
67      <include>openbsd_rules.xml</include>
68      <include>clam_av_rules.xml</include>
69      <include>bro-ids_rules.xml</include>
70      <include>dropbear_rules.xml</include>
71      <include>local_rules.xml</include>
72    </rules>
73
74    <syscheck>
75      <!-- Frequency that syscheck is executed - default to every 22 hours -->
76      <frequency>300</frequency>
77
78      <!-- Directories to check  (perform all possible verifications) -->
79      <directories check_all="yes">/etc,/usr/bin,/usr/sbin</directories>
80      <directories check_all="yes">/bin,/sbin</directories>
81
82      <!-- Files/directories to ignore -->
83      <ignore>/etc/mtab</ignore>
84      <ignore>/etc/mnttab</ignore>
85      <ignore>/etc/hosts.deny</ignore>
86      <ignore>/etc/mail/statistics</ignore>
87      <ignore>/etc/random-seed</ignore>
88      <ignore>/etc/adjtime</ignore>
                    Plain Text   Tab Width: 8   Ln 76, Col 19      INS
```

```
[alice@sunshine  ossec-hids-2.7]# /var/
ossec/bin/ossec-control start
```

الآن البرامج المكونة لنظام (OSSEC) تعمل، ويمكنك عرض سجل نظام (OSSEC) من خــلال الدليل (var/ossec/logs/ossec .log/). ويقدم لك هذا الســجل تفاصيل بالملفات التــي يقرؤها نظام (OSSEC) أثناء بدء التشــغيل، كما يعرض لــك نتائج تنفيذ البرامج في نظام (OSSEC). وعند اكتشــاف نظــام (OSSEC) أي حالة تكون خطيرة من جهة أمنية فإنــه يتم تســجيل التفاصيل في الدليــل (var /ossec/logs/alerts/alerts. conf/). لكن مُخرجات نظــام (OSSEC) عبارة عن كميات كبيرة من المعلومات، وعرض تلك المعلومات من خلال تصفح الســجل ليس بالأمر السهل. وفي المقابل، فإن حزمة (OSSEC-WebUI) وهــي واجهة معتمدة على الشــبكة، تقدم طريقة أســهل بكثير للبحــث ولعرض تنبيهات السجل (الشكل ٩-٩).

وخلافاً لحزمة نظام (OSSEC) الرئيســية، فإن حزمــة (OSSEC-WebUI) لا تتضمن النــص البرمجــي الخاص بالتثبيت، ومن ثــم فإن هذه الحزمة تحتــاج إلى مزيد من الجهد لإعداد التهيئة.

```
[root@sunshine]# cd /home/shared/busi-
ness_finance/information_technology/
website/main
[root@sunshine main]# cp /opt/book/con-
trols/packages/ossec-wui-0.3.tar.gz .
[root@sunshine main]# tar zxvf ossec-wui-
0.3.tar.gz
[root@sunshine main]# mv ossec-wui-0.3
ossec
[root@sunshine main]# groupmems -g ossec
-a apache
[root@sunshine main]# chmod 777 /tmp
[root@sunshine main]# chmod 770 /var/
ossec/tmp
[root@sunshine main]# chgrp apache /var/
ossec/tmp
[root@sunshine main]# service httpd
restart
```

ويُفـترض الآن أن تكون قادراً على الوصـول إلى واجهة (OSSEC-WebUI) عن طريق فتح متصفح الشبكة وزيارة موقع (http://sunshine.edu/ossec).

ولاختبار أن نظام (OSSEC) يعمل بشـكل صحيح، سـتقوم الآن بتطبيق بعض الطرق التي يُستخدم فيها نظام (OSSEC) لمراقبة الحوادث الأمنية المُحتملة.

مراقبة تكامل الملفات:

يقـوم برنامـج مراقبة تكامل الملفات في نظام (OSSEC) بالكشـف عـن التغييرات في ملفـات النظـام ويُنبهك عند حدوثهـا. ويمكن أن يحدث ذلك بسـبب هجوم خارجي، أو

إساءة استخدام من مستخدم داخلي، أو حتى بسبب خطأ مطبعي من قبل أحد المسؤولين. ولمحــاكاة إحدى الهجمات التي تقوم بتعديل ملفات النظام، ســتقوم بتعديل أحد الملفات وستعرض النتائج في نظام (OSSEC-WebUI).

الشكل (٩-٩): واجهة نظام (OSSEC-WebUI)

١. عدل محتويات الدليل التالي (/ etc/hosts) للتطابق مع ما يلي:

```
127.0.0.1 sunshine.edu localhost hacked.
sunshine.edu
::1  sunshine.edu localhost
```

٢. انتظــر ٥ إلى ١٠ دقائــق لأن اختبــار تكامل الملفات يعمل كل خمــس دقائق، لكن قد يستغرق بعض الوقت لاســتكمال العملية لذا من الأفضل الانتظار لبضع دقائق للتأكد من اكتمال عملية المسح.

٣. افتح نظام (OSSEC-WebUI) واختر علامة التبويب (Integrity checking).

٤. انقر على علامة الجمع المجاورة لدليل (/etc/hosts) لمعرفة تفاصيل حول هذا الملف.

٥. خذ لقطة من الشاشة لهذه الصفحة وقم بتسليمها لأستاذ المادة.

مراقبة السجل:

يقوم نظام (OSSEC) بتجميع وتحليل وربط سـجلات متعددة من نظام لينكس وذلك لإخبار المسـتفيد بما يحدث. ولتطبيق ذلك سـتقوم ببعض مهام إدارة النظام الشائعة التي تُنتج رسائل تدقيق يمكن تتبعها بنظام (OSSEC) ومن ثم عرض النتائج.

١. قم بتثبيت حزمة (zsh) باستخدام مدير الحزم (YUM).

٢. قم بإنشاء مستخدم جديد

اسم المستخدم: ossec-sample

الدليل الرئيسي: /home/ossec-sample

كلمة المرور: oSS3c!

٣. افتح نافذة طرفية وقم بتشغيل الأمر التالي:

```
[alice@sunshine ~]$ ssh bob@sunshine.edu
```

٤. عند المطالبة بكلمة مرور، استخدم (bisforbanana).

٥. افتح نظام (OSSEC-WebUI) باستخدام متصفح الإنترنت.

٦. انتظر ٥ إلى ١٠ دقائق حتى يكمل نظام (OSSEC) عمليات المسح.

٧. قـم بمراجعة التنبيهات الأخيرة التي التقطها نظام (OSSEC) وحدد تلك التنبيهات المتعلقة بالأحداث الثلاثة أعلاه.

٨. قم بنسخ ولصق بيانات كل حدث في مستند وورد.

النتائج المطلوب تسليمها: قم بتسليم المستند الذي يحتوي على نتائج نظام (OSSEC) إلى أستاذ المادة.

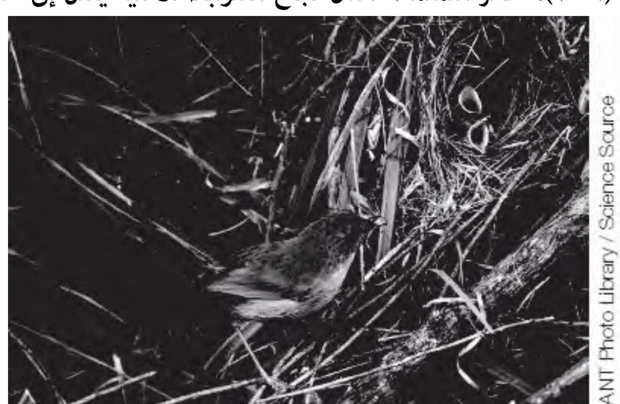
تمرين التفكير النقدي - ضوابط أمنية تتعدى الإطار البشري:

في شـــهر نوفمبر من عام ٢٠١٢، اقترحت بعض البحوث الأسترالية أنه بالإمكان استخدام الضوابط الأمنية بطرق مثيرة للاهتمام خارج العالم البشري للتعامل مع المشـــكلات الفريدة في الحفاظ على الحياة البرية. على سبيل المثال، طائر الوقواق البرونزي يضع بيضه في عش طائر النمنمة على أمل أن يترك واجبات الاهتمام بصغاره إلى طائر النمنمة الغافل بسبب أن بيض هذين النوعين من الطيور متشابه إلى حد كبير مما يتيح القيام بهذه الحيلة.

من وجهة نظر طائر النمنمة فإن المشـــكلة في الواقع أســـوأ من ذلك بكثير. فبيض طائر الوقـــواق يفقس قبـــل بيض طائر النمنمة بثلاثة أيام، أي ١٢ يوم في مقابل ١٥ يوم. وبمجرد خـــروج فراخ الوقواق من البيـــض فإنها تدفع بيض طائر النمنمـــة إلى خارج العش. ودون وجود آلية اكتشـــاف فعالة، فإن طائر النمنمة المتضرر قـــد ينتهي به الأمر إلى إطعام فراخ الوقواق السيئة التي حطمت بيضه.

وبينـــما يكون طائر النمنمة غير قادر على فعل الكثير لمنع تدمير بيضه، إلا أنه قد وضع آلية (وســـيلة ضبط) لتجنب إطعـــام طائر الوقواق. بعد ١٠ أيام مـــن وضع طائر النمنمة للبيـــض تبدأ الأم بالغناء لأجنتها التي لا تـــزال في بيضها. وبعد خروجها من بيضها فإنه من المتوقـــع أن تُدرج الفراخ الإيقاعات المميزة للأغنية أثناء طلبها للطعام. فإذا لم تســـمع الأم الإيقاعات المميزة للأغنية فإنه ســـيتم التخلي عن تلك الفراخ. وتحصل أجنة طائر النمنمة عـــلى ٥ أيام لتعلم الإيقاعـــات المميزة للأغنية في حين تحصل أجنة طائر الوقواق على يومين فقط، وهي فترة غير كافية لتعلم الإيقاعات المميزة للأغنية. إن نسبة نجاح هذا الاختبار في الكشف عن الطائر الشرير قرابة (٤٠٪) (شكل ٩-١٠).

الشكل (٩-١٠): طائر النمنمة، معدل نجاح الضوابط الأمنية يصل إلى ٤٠٪



المراجع:

Schneier, B. Cryptogram, November 15, 2012

Yong E., «Fairy Wrens teach secret passwords to their unborn chicks to tell them apart from cuckoo impostors,» Discover Magazine blog, November 8, 2012, http://blogs.discovermagazine.com/notrocketscience/2012/11/08/fairy-wrens-teach-secret-passwords-to-their-unborn-chicks-to-tell-them-apart-from-cuckoo-impostors (accessed 07/18/2013)

Corbyn, Z. «Wrens teach their eggs to sing,» November 8, 2012, http://www.nature.com/news/wrens-teach-their-eggs-to-sing-1.11779 (accessed 07/18/2013)

أسئلة على تمرين التفكير النقدي:

١. من بين الضوابط الأمنية التي ناقشناها في هذا الفصل، أي الضوابط يُشبه إلى حد كبير وسيلة الضبط المُستخدمة من قبل أنثى طائر النمنمة في اكتشاف المخادعين؟

٢. وسيلة الضبط المُستخدمة من قبل أنثى طائر النمنمة تبدو معقدة نوعاً ما. يوجد بعض الضوابط الأبسط التي تتحدث عن نفسها. هل بإمكانك أن تذكر بعضاً منها؟

تصميم حالة:

طُلب منك أن تقوي الجانب الأمني لآلة (CentOS) لأحد أعضاء هيئة التدريس. وهذا العضــو قد حصل على منحة كبيرة من الحكومة الاتحادية، وهذه المنحة تتطلب اســتخدام آلة (CentOS) لتحليل بعض البيانات. وتُعد النتائج بيانات مقيدة لذا يعد الوصول لجهاز الحاسب الآلي مقيداً أيضاً. إنك لست متأكداً كيف ستقوم بذلك لذا قمت ببعض البحث.

وبعــد القيام بالبحث على شــبكة الإنترنت، وجدت البنــود المُدرجة من ١ إلى ٦ أدناه. اكتب الإجــراءات المُحددة (مجموعة الأوامر وتفاصيل الملفات) التي ستســتخدمها لتنفيذ هذه التغييرات بحيث يمكنك تكرارها على أجهزة أخرى حسب الحاجة.

١. قم بتغيير المنفذ الافتراضي لـ (sshd) من المنفذ (٢٢) إلى المنفذ (٤٤٤٤). بهذا التغيير البسيط سوف نتفادى أكثر المسوح الآلية الموجهة لاقتحام الجهاز باستخدام (SSH).

٢. أضف مُعرف تسجيل الدخول لعضو هيئة التدريس (jamesc) إلى مجموعة العجلة (wheel group).

٣. قم بتعطيل تســجيل دخول (SSH) كجذر، وذلك لإجبار المستخدمين على استخدام أمر (sudo). هذا الأمر يســمح للمســتخدمين المدرجــين في مجموعة العجلة برفع امتيازاتهم وتنفيذ الأوامر مثل مستخدم الجذر.

٤. قم بتغيير معايير عمر كلمات المرور للمســتخدم (jamesc) وذلك لتنتهي خلال ٦٠ يوماً.

٥. قم بتغيير المعايير التاريخية لكلمات المرور وذلك لاســتعادة آخر ثلاث كلمات مرور، ولجعل الحد الأدنى لطول كلمات المرور ثمانية رموز.

٦. اذكر قواعد الجدار الناري واحتفظ بنسخة ورقية منها.

تلميح: قد تجد ملفات التهيئة والأوامر التالية مفيدة:

- sshd_config
- login.defs
- group
- chage
- system-auth
- iptab

الفصل العاشر

البرمجة النصية لقشرة نظام التشغيل

نظرة عامة:

ناقشنا في الفصول السابقة بعض المهام الشائعة المرتبطة بإدارة النظام. في الفصل الثاني مــن هــذا الكتاب بدأنا بمقدمة حول دور مســؤول النظام، ثم ناقشــنا في الفصول اللاحقة الضوابط التقنية المســتخدمة في مكافحة التهديدات الأمنية والجهود المطلوبة عند حدوث اختراق أمني.

في هــذا الفصل ســنناقش طريقة للتعامل مــع المهام المعقدة، والمطلوبــة لإدارة فعالة للنظــام، والمتكــررة في كثير من الأحيان. وتقدم «قشرة باش» (BASH shell)، وهي قشرة نظام التشغيل، آلية لإنشاء نص برمجي هو تطبيق مركب من عدة تطبيقات لسطور الأوامر، وذلك لإنجاز المهام المعقدة. في نهاية هذا الفصل يجب أن تعرف:

- كيفية كتابة نص برمجي بسيط لقشرة نظام التشغيل (BASH).
- استخدام عناصر البرمجة الشائعة (المتغيرات، والحلقات، وغيرها).
- كيفية التعامل مع تفاعل المستخدم.
- كيفية استخدام أدوات نظام ينكس الشائعة لتحليل ومعالجة الملفات النصية.

مقدمة:

تُعد المعرفة الأساســية بالبرمجة النصية لقشرة نظام التشغيل أمراً ضرورياً لكل من يريد اســتكمال مهام إدارة النظام الشائعة، أو تدقيق أمن النظام، أو تطبيق الكثير من الضوابط التي ناقشــناها في الفصول السابقة. وتُستخدم النصوص البرمجية لقشرة نظام التشغيل في أتمتة العمليات في نظام ينكس بدءاً من تشغيل خدمات الشبكات عند بدء تشغيل النظام، ووصولاً إلى تهيئة بيئة قشرة نظام التشغيل التابعة للمستخدم أثناء تسجيل الدخول. ويمثل

هذا الفصل مقدمة للبرمجة النصية لقشرة نظام التشـغيل. وللبدء في هذا الفصل سـنقوم بإنشـاء نصوص برمجية تكون أمثلة على الإجراءات والهياكل الشائعة الاستخدام في البرمجة النصية لقشرة نظام التشغيل. وفي الأجزاء اللاحقة من هذا الفصل سنقوم بدمج بعض هذه العناصر الشائعة لتوضيح أتمتة العمليات التي تستغرق وقتاً طويلاً جداً للقيام بها يدوياً، أو تلك التي تحتاج إلى تكرارها في المستقبل.

ما هو بالضبط النص البرمجي وكيف يختلف عن البرامج المكتوبة بلغات البرمجة الأخرى والتـي قـد تكون معروفة لديك مثـل لغة الجافا (Java) ولغة السـي (C#)؟ الفرق الأهم بـين النص البرمجي والبرنامج المكتوب بلغات البرمجـة الأخرى مثل الجافا هو أن النصوص البرمجية لا يجب تجميعها في ملف ثنائي الصيغة ليتم تشغيلها، إذ يتم تفسير النص البرمجي وتحويله إلى الصيغة الثنائية اللازمة في وقت التشـغيل. وبما أنه تم الاسـتغناء عن عملية التجميـع في البرمجـة النصية، فإن تطوير التطبيقات باسـتخدام لغة البرمجة النصية يكون بشـكل عام أسرع من تطويرها باسـتخدام اللغات التي تعتمد على عملية التجميع. لكن قد يكون هناك تأثير في الأداء عند تنفيذ التعليمات البرمجية حيث يوجد العديد من لغات البرمجـة النصية الشـائعة مثل لغـة (PHP)، ولغة (Python)، ولغـة (Ruby). وبعكس البرامج النصية المكتوبة بهذه اللغات، فإن البرامج النصية لقشرة نظام التشغيل لا تحتاج إلى برنامج مُفسر لتحويل النص البرمجي إلى صيغة ثنائية. ويتم تفسـير النص البرمجي لقشرة نظام التشغِيل مباشرة بواسطة عملية قشرة نظام التشغيل، وهي قشرة (BASH) في حالتنا هذه، إلا أنه يمكن استخدام أي نوع من أنواع قشرة نظام التشغيل السائدة.

لغة البرمجة النصية لنظام ويندوز (Windows Powershell)

منذ الإصدار السـابع لويندوز٧ (Windows 7) قامت مايكرسـوفت بإطـلاق لغة برمجة نصية جديـدة تُدعـى (Powershell) والتي لا تحتوي على المكونات البرمجية التي سنناقشـها في هذا الفصل فحسـب بل تحتوي على أكثر من ذلك بكثير. وقامت مايكروسـوفت بدمج وظائف لغة البرمجة النصية (Powershell) في أنظمتها التشـغيلية وذلك للسـماح لمسؤول النظام بالوصول العمـلي إلى أي وظيفية من وظائف ويندوز، سـواء كانت تلـك الوظيفة محلية أم على الأنظمة البعيدة.

لـن نقوم في هذا الكتاب بتغطية موضوع لغة البرمجـة النصية (Powershell)، لكن لمزيد من المعلومـات حول هذا الموضوع، يمكن زيـارة (Microsoft Script Center) على الرابط التالي:
http://technet.microsoft.com/scriptcenter

إذاً كيف نكتب نصاً برمجياً لقشرة نظام التشـغيل؟ النص البرمجي لنظام التشـغيل في أبسـط أشـكاله هو قائمة من الأوامر المحفوظة في ملف نصي والتي نسـتطيع تشغيلها من خلال استدعاء برنامج (BASH) الموجود في سطر الأوامر:

قائمة ١: (/opt/book/scripting/backup_v1)

```
[alice@sunshine ~]$ cat /opt/book/scripting/backup_v1
mkdir -p /tmp/backups
cp -pr /home/alice/work /tmp/backups
cd /tmp/backups/
zip -qr backup.zip work/
rm -rf /tmp/backups/work

echo «Done Backing up the work directory»
[alice@sunshine ~]$ bash /opt/book/scripting/backup_v1
Done Backing up the work directory
[alice@sunshine ~]$ ls /tmp/backups
backups.zip
```

وهـذا يوفر عليـك جهد إعادة كتابة قائمة من الأوامر في كل مرة تحتاج فيها إلى لإكمال المهمة. لكن من خلال إضافة سطر واحد إلى أعلى النص البرمجي ومن خلال تغيير أذونات الملف لجعله قابلاً للتنفيذ، نستطيع تحويل قائمة الأوامر هذه إلى أمر قائم بذاته:

قائمة ٢: (/opt/book/scripting/backup_v1)

```
#! /bin/bash
# This is a comment.
# Lines starting with the pound sign (#) are ignored in BASH scripts
#
# This script copies and compresses files in /home/alice/work and
# saves them to /tmp/backups/work
mkdir -p /tmp/backups
cp -pr /home/alice/work /tmp/backups
cd /tmp/backups/
zip -qr backup.zip work/
rm -rf /tmp/backups/work
echo «Done Backing up the work directory»

[alice@sunshine ~]$ chmod 500 /opt/book/scripting/backup_v2
[alice@sunshine ~]$ /opt/book/scripting/backup_v2
Done Backing up the work directory
```

الأمـر (chmod) يقوم بتعيـين البت (bit) القابل للتنفيذ لصاحـب الملف، والبقية لن يكونـوا قادرين على تنفيذ النص البرمجي. السـطر الأول مـن هذا الإصدار للنص البرمجي (#!/bin/bash) يُخـبر نظام التشـغيل بأن هـذا الملف يجب إرسـاله إلى البرنامج المحدد للمعالجة. كما قمنا أيضاً بإضافة ملاحظة على هذا النص البرمجي. إن أي سطر يبدأ بعلامة (#) فـإن (مُفسر بـاش) (BASH interpreter) يقوم بتجاهله ومـن ثم يعده ملاحظة أو تعليقاً. وتساعد الملاحظات على توثيق كيفية عمل النص البرمجي خصوصاً إذا كان المنطق المستخدم معقداً نوعاً ما. وتستطيع إضافة ملاحظة لشرح ما تقوم به عبارة معينة وتوضيح الناتج المتوقع منها. كما تسـمح لك الملاحظات بإضافة معلومات مهمة عن النص البرمجي مثل اسم المُبرمج وتاريخ آخر تعديل.

وبمجـرد إضافة هذا السـطر إلى أعلى الملف النصي، تسـتطيع تعيـين الأذونات لجعل الملف قابلاً للتنفيذ مما يؤدي إلى إنشاء تطبيق مخصص وجديد. وتستطيع استخدام هذه

الخطوات لإنشـاء نص برمجي لأي مجموعة من الأوامر التي تحتاج إلى تكرار على أسـاس منتظـم. كما أن طول قائمة الأوامر ليس مهـماً، إذ يمكن أن يكون لديك قائمة تحتوي على مائة أمر أو قائمة تحتوي على أمر واحد فقط. وعادة ما يكون من الجيد أن تُنشَـأ نصوص برمجية لأمر واحد إذا كانت خيارات سـطر الأوامر المتعددة مطلوبة لإنجاز المهمة كما هو الحال مع الأمر (curl) والأمر (wget).

إعادة توجيه المخرجات:

لقـد رأينا كيفية حفـظ برامج متعددة في ملف نص برمجـي واحد، لكن هناك طريقة أخرى لدمج بعض برامج سطر الأوامر لتنفيذ مهام معقدة. ويمكن استخدام مخرجات الأمر الأول لتكون مدخلات للأمر الثاني، مما يؤدي إلى إنشـاء ما يرقى إلى نص برمجي في سـطر واحد. وهذا ممكن لأن هيكلة نظام ينكس تستخدم التيارات (streams). والتيار «ما هو إلا سلسـلة من البايتات التي يمكن قراءتها أو كتابتها باسـتخدام وظائف المكتبة البرمجية التي تُخفي تفاصيل الجهاز المستخدم عن التطبيق البرمجي. والبرنامج نفسه يمكنه الكتابة أو القراءة من وحدة طرفية، أو ملف، أو منفذ شبكة بطريقة مستقلة عن الجهاز باستخدام التيارات»[1]. وهناك ثلاثة أنواع من التيارات الموحدة للمدخلات والمخرجات:

- مدخلات موحدة (stdin) وتعمل على تقديم مدخلات من لوحة المفاتيح.
- مخرجات موحدة (stdout) وتعمل على عرض مخرجات الأوامر على الشاشة.
- الأخطاء الموحدة (stderr) وتعمل على عرض رسائل الأخطاء على الشاشة.

ويمكـن إعادة توجيـه تيارات المدخـلات والمخرجات بسـهولة في قشرة نظام التشـغيل (BASH) مما يسمح بقراءة المدخلات من الملف بدلاً من لوحة المفاتيح، وإرسال واحد أو أكثر من تيارات المخرجات لبرنامج آخر كمدخلات، وحفظ المخرجات في ملف. ويربط عامل النقل (|) (pipe operator) بين تيار (stdout) لأحد البرامج بتيار (stdin) لبرنامج آخر. ومثالاً على ذلك سنذكر قائمة الأوامر في (/user/bin) التي تحتوي على كلمة (gnome) في اسم الملف:

---

(1) Shields, I. N.p.. Web. 10 December 2012, <http://www.ibm.com/developerworks/library/l-lpic1-v3-103-2/>

```
[alice@sunshine ~]$ ls -l /usr/bin | grep gnome
```

فعندمــا تقوم بتشــغيل هذا الأمر ســوف تتلقى نحــو ٥٠ ملفاً نتيجة لهــذا الأمر. ما الذي ســتفعله إذا كنت ترغب في الحصول عــلى النتائج الثلاث الأولى فقط؟ بإمكانك نقل المخرجات من أمر (grep) إلى أمر آخر:

```
alice@sunshine ~]$ ls -l /usr/bin | grep gnome | head -3
-rwxr-xr-x.  1 root root  37070 Mar 20 2012 gnome-about
-rwxr-xr-x.  1 root root  88944 Jun 25 10:29 gnome-about-me
-rwxr-xr-x.  1 root root 233664 Jun 25 10:29 gnome-appearance-properties
```

عامل إعادة التوجيه (>) يُســتخدم لإرســال المخرجات إلى ملف بــدلاً من عرضها على الشاشة. ويمكنك أيضاً إلحاق البيانات إلى ملف موجود باستخدام عامل (>>):

```
[alice@sunshine ~]$ ls -l /usr/bin | grep gnome | head -3 > /tmp/exam-
ple.txt
[alice@sunshine ~]$ cat /tmp/example.txt
-rwxr-xr-x.  1 root root    37070 Mar 20 2012 gnome-about
-rwxr-xr-x.  1 root root    88944 Jun 25 10:29 gnome-about-me
-rwxr-xr-x.  1 root root  233664 Jun 25 10:29 gnome-appearance-properties
[alice@sunshine ~]$ ls -l /usr/bin | grep gnome | head -5 >> /tmp/
example.txt
[alice@sunshine ~]$ cat /tmp/example.txt
-rwxr-xr-x.  1 root root   37070 Mar 20 2012 gnome-about
-rwxr-xr-x.  1 root root   88944 Jun 25 10:29 gnome-about-me
-rwxr-xr-x.  1 root root 233664 Jun 25 10:29 gnome-appearance-properties
-rwxr-xr-x.  1 root root   37070 Mar 20 2012 gnome-about
-rwxr-xr-x.  1 root root   88944 Jun 25 10:29 gnome-about-me
-rwxr-xr-x.  1 root root 233664 Jun 25 10:29 gnome-appearance-properties
```

إن اســتخدام برامــج صغيرة ومتعــددة على التوالي بــدلاً من اســتخدام تطبيق واحد ومعقد أمر أساسي في تصميم نظام ينكس. وقد لخص المطور الأساسي لنظام إعادة توجيه المدخــلات والمخرجات في ينكس، دوغ ماكلــوري (Doug McIlroy)، ذلك بهذه الطريقة: «هذه فلســفة نظــام ينكس: كتابة برامج تقوم بأداء شيء واحــد لكنها تقوم به بالطريقة الصحيحــة. كتابة البرامج التي تعمل معــاً. كتابة البرامج التي تتعامل مع التيارات النصية لأن ذلك يعدّ واجهة شاملة»[٢].

معالجة النص:

ولأن اســتخدام ومعالجة تيارات النصوص مهــم جداً لكتابة النص البرمجي لقشرة نظام التشــغيل، سوف نقضي بعض الوقت لمناقشة تطبيقات سطر الأوامر المتخصصة في معالجة تيــارات النصــوص. وهــذه الأوامر مع بعضها البعض تشــبه إلى حد كبير «ســكين الجيش الســويسري» الخاصة بمعالجة التيــارات النصية لأنها توفر كل شيء بــدءاً من فرز الملفات ووصــولاً لتحويــل الحالات، كما أنها تُســتخدم تقريباً في كل نص برمجــي بغض النظر عن حجمه.

أمر القص (Cut):

ستجد نفسك تتعامل غالباً مع بيانات عمودية تستخدم شكلاً من أشكال الفواصل، مثل علامــة التبويب أو الفاصلــة، وذلك لتحديد كل عمود في مجموعة البيانات. ويســمح لك أمر القص (cut) بتحليل كل سطر في ملف البيانات ومن ثم استخراج عمود البيانات الذي تحتاج إليه فقط.

وفي هذا المثال سنستخدم ملف جداول البيانات إكسل الذي يحتوي على بيانات مفصولة بفواصل (Comma-Separated Value) (CSV)، كما يحتوي على الحقول التالية: الاســم الأول، واســم العائلة، واســم المســتخدم، وعنوان البريد الإلكتروني. ويمكن استخراج البريد الإلكتروني لجميع المستخدمين من خلال ما يلي:

(2) Peter, S. A Quarter-Century of Unix, Addison-Wesley, 1994

```
[alice@sunshine ~]$ head -3 /opt/book/scripting/users.csv
Ian,Cook,ian.cook,ian.cook@sunshine.edu
Christine,Riggs,christine.riggs,christine.riggs@sunshine.edu
Lindsay,Fishbein,lindsay.fishbein,lindsay.fishbein@sunshine.edu
[alice@sunshine ~]$ cut -d, -f4 /opt/book/scripting/users.csv
ian.cook@sunshine.edu
christine.riggs@sunshine.edu
lindsay.fishbein@sunshine.edu
. . .
```

كما نســتطيع إرجاع الأعمدة المتعددة وتصفيــة المخرجات وذلك بدمج أمر (cut) بأمر (grep):

```
[alice@sunshine ~]$ cut -d, -f1,2,4 /opt/book/scripting/users.csv |
grep john
John,Jayavelu,john.jayavelu@sunshine.edu
Jennifer,Johnson,jennifer.johnson@sunshine.edu
John,Altier,john.altier@sunshine.edu
```

وكما ترى فإنه تم اســتعادة العمــود الأول والعمود الثاني والعمود الرابع، كما تم عرض السجلات التي تحتوي فقط على نص «john».

أمر الفرز (Sort):

أمر الفرز (sort) يقوم بما يدل عليه مُسماه-يقوم بفرز سطور الملف النصي:

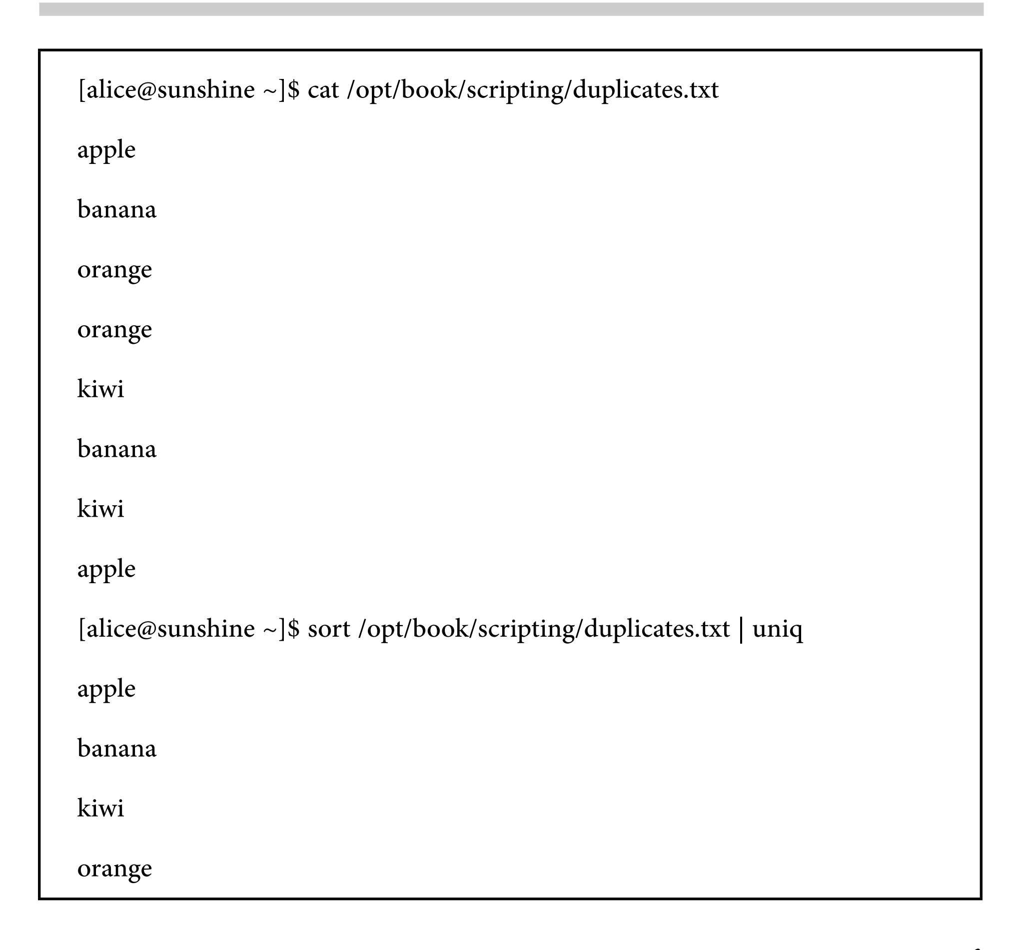
```
[alice@sunshine ~]$ cat /opt/book/scripting/words.txt
eyes
record
explosive
spice
prison
videotape
leg
ice
magnet
printer
[alice@sunshine ~]$ sort /opt/book/scripting/words.txt
explosive
eyes
ice
leg
magnet
printer
prison
record
spice
videotape
```

ونلفــت الانتبــاه إلى أن ترتيب الفرز الافتراضي قائم على أســاس البيانات النصية، لذلك يجب استخدام المفتاح (n-) في حال فرز البيانات الرقمية:

```
[alice@sunshine ~]$ sort /opt/book/scripting/numbers.txt
1
1002
1234567
356
4
8675309
99
[alice@sunshine ~]$ sort -n /opt/book/scripting/numbers.txt
1
4
99
356
1002
1234567
8675309
```

أمر إزالة السطور المكررة (uniq):

وبمواصلة الحديث عن الأوامر البسـيطة التي يدل مُسـماها عـلى وظيفتها، فإن الأمر (uniq) يقوم بإزالة السـطور المكررة من الملف النصي. ويقوم الأمر (uniq) بالبحث فقط في السطور المجاورة للعثور على التكرار لذا يجب في البداية فرز المدخلات.



```
[alice@sunshine ~]$ cat /opt/book/scripting/duplicates.txt
apple
banana
orange
orange
kiwi
banana
kiwi
apple
[alice@sunshine ~]$ sort /opt/book/scripting/duplicates.txt | uniq
apple
banana
kiwi
orange
```

أمر الاستبدال (tr):

يقوم الأمر (tr) باستبدال قائمة محددة من الرموز بمجموعة أخرى من الرموز، أو يقوم بحــذف تلك الرمــوز (-d) من تيار المدخلات. ويمكن اســتبدال الحــروف (x) و(y) و(z) بالحروف (a) و(b) و(c) عند وجودها في ملف نصي من خلال ما يلي:

```
alice@sunshine ~]$ cat /opt/book/scripting/original.txt
The quick brown fox jumps over the lazy dog.
[alice@sunshine ~]$ cat /opt/book/scripting/original.txt | tr «abc»
«xyz»
The quizk yrown fox jumps over the lxzy dog.
[alice@sunshine ~]$ cat /opt/book/scripting/original.txt | tr -d
«abc»
The quik rown fox jumps over the lzy dog.
```

والوظيفة الأكثر شـيوعاً للأمـر (tr) هي تحويل الحروف الصغـيرة في النص إلى حروف كبيرة وبالعكس:

```
alice@sunshine ~]$ cat /opt/book/scripting/original.txt | tr «[:lower:]»
«[:upper:]»
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG.
```

وتُعد المجموعات [:Iower:] و[:upper:] من مجموعات الرموز، وهي عبارة عن طريقة سريعـة لتحديد جميع الحروف الصغيرة والكبيرة عـلى التوالي. وللحصول على قائمة كاملة لمجموعات الرموز، انظر صفحة الأمر (tr) في دليل الأوامر (man tr).

المتغيرات:

المتغـير هو تمثيل لجزء من البيانات (رقم، اسـم الملف، نص، وغيرها) محفوظ في ذاكرة جهاز الحاسب الآلي. ولإنشاء متغير جديد نحتاج فقط إلى اسم المتغير والبيانات التي يمثلها: قيمة تلك البيانات.

```
[alice@sunshine ~]$ myVariable=20
[alice@sunshine ~]$ echo $myVariable
20
```

ولا يسمح بالمسافات بعد أو قبل علامة يساوي (=) عند تعيين قيمة المتغير. ولذلك فإن نتيجة العبارات التالية كلها ستكون خاطئة:

```
[alice@sunshine ~]$ myVariable = 20
[alice@sunshine ~]$ myVariable =20
[alice@sunshine ~]$ myVariable= 20
```

ويمكنك أيضاً تعيين نص أو متغير آخر كقيمة للمتغير.

```
[alice@sunshine ~]$ hello=«Hello World»
[alice@sunshine ~]$ world=$hello
[alice@sunshine ~]$ echo $hello
Hello World
[alice@sunshine ~]$ echo $world
Hello World
```

وأخـيراً يمكنك تعيـين مخرجات أحد الأوامـر كقيمة للمتغير وذلك مـن خلال تضمين الأمر باسـتخدام القوسـين وعلامة الدولار $()، والمعروفة باسـم تمديد الأمر (command expansion).

```
[alice@sunshine ~]$ now=$(date)
[alice@sunshine ~]$ echo $now
Wed Dec 19 10:41:40 EST 2012
```

الجدول (١٠-١): العوامل الحسابية في قشرة نظام التشغيل (Bash)

العامل	الوصف	مثال	النتيجة
+	جمع	$((٥+٥))	١٠
-	طرح	$((٥-١))	٤
*	ضرب	$((٣*٢))	٦
/	قسمة	$((١٠/٢))	٥
٪	المعامل (الباقي)	$((١٠٪٣))	١
**	الأس	$((٦**٢))	٣٦

كـما يمكنك أيضاً القيام بالعمليات الحســابية الأساسـية للأعـداد الصحيحة (أرقام من دون كسور) في قشرة نظام التشغيل (BASH) وذلك باستخدام $((   )) والتي تشــير إلى التمديد الحسابي (arithmetic expansion). ويوضح الجدول (١٠-١) قائمة بالعمليات الحسابية التي يمكن القيام بها في قشرة نظام التشغيل (BASH).

```
[alice@sunshine ~]$ myVariable=20
[alice@sunshine ~]$ myBigVariable=$(( $myVariable * 100 ))
[alice@sunshine ~]$ echo myBigVariable
2000
[alice@sunshine ~]$ echo $(( $myBigVariable + 1 ))
2001
```

الاقتباس (Quoting):

وضـع المتغـير بين علامتـي تنصيص («») لا يؤثر في اسـتعماله. لكن اسـتخدام علامة التنصيص المفردة (‹›) يؤدي إلى استخدام اسم المتغير حرفياً بدلاً من استبدال قيمة المتغير.

قائمة ٣: (/opt/book/scripting/quoting):

```
#! /bin/bash
name=Alice
echo «My name is $name and the date is $(date +%m-%d-%Y)»
echo 'My name is $name date is $(date +%m-%d-%Y)'


[alice@sunshine ~]$ /opt/book/scripting/quoting
My name is Alice and the date is 122012-19-
My name is $name and the date is $(date +%m-%d-%Y)
```

وكما ترى فإن اســتخدام علامة التنصيص المفردة في الســطر الثاني أدى إلى كتابة أسماء المتغير حرفياً، في حين أن استبدال المتغير تم في السطر الأول. ولاحظ أيضاً أن التاريخ الحالي تم اســتبداله بـ (date +٪m-٪d-٪ Y)$ دون الحاجة إلى تعيين اسم المتغير. ويتم تشغيل الأوامــر المتضمنة في ()$ في كل مرة يتم التعرض لهــا في النص البرمجي، وبذلك يتم تحديد القيمة بشكل متجدد.

متغيرات البيئة:

بعض المتغيرات تُنشَــأ آلياً عند تســجيل الدخول أو عند البدء في نافذة طرفية جديدة. وهــذه المتغــيرات البيئيــة تحتفظ بقيــم افتراضية وتحتفــظ كذلك بتفضيــلات افتراضية للمســتخدم في الجلســة الحالية. ويمكن عرض قائمة بمتغيرات البيئــة وقيم تلك المتغيرات باستخدام الأمر (env):

```
[alice@sunshine ~]$ env
HOSTNAME=sunshine.edu
SHELL=/bin/bash
USER=alice
PATH=    (/usr/lib/qt-3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/
sbin:/usr/sbin:/sbin:/home/alice/bin
…
PWD=/home/alice
TERM=xterm
```

وفي النتائج سترى عدة شاشات من البيانات، ومعظم تلك البيانات لها علاقة بالتطبيقات، لكن هناك بعض المتغيرات التي تستحق الذكر (الجدول ١٠-٢).

ويمكن استخدام هذه المتغيرات في سطر الأوامر تماماً مثل المتغيرات العادية:

```
alice@sunshine ~]$ echo «My name is $USER and my current directory is
$PWD»
My name is alice and my current directory is /home/alice
```

كما يمكننا الاســتفادة من هذه المتغيرات في البرمجة النصية لقشرة نظام التشغيل. على سبيل المثال، انظر القائمة (٤):

قائمة ٤: (opt/book/scripting/env_variable_example):

```
#! /bin/bash
echo «Hello $USER»
echo «You are calling this program from $PWD»
echo «Your home directory is $HOME»
```

ولأن متغيرات البيئة تُنشَــأ آلياً بواســطة قشرة نظام التشغيل (BASH)، فسيكون لدينا مخرجات متجددة تعتمد على المســتخدم الذي ينفذ النص البرمجي. وهنا تجد المخرجات عندما قامت أليس (Alice) بتشغيل النص البرمجي:

```
[alice@sunshine Desktop]$ /opt/book/scripting/env_variable_example
Hello alice
You are calling this program from /home/alice/Desktop
Your home directory is /home/alice
```

وهنا تجد المخرجات عندما قام بوب (Bob) بتشغيل النص البرمجي:

```
[bob@sunshine tmp]$ /opt/book/scripting/env_variable_example
Hello bob
You are calling this program from /tmp
Your home directory is /home/bob
```

الجدول(١٠-٢): قائمة بالمتغيرات البيئية الشائعة

المتغير	الوصف
USER	المستخدم الحالي
HOME	الدليل الرئيسي للمستخدم الحالي
PWD	الدليل الحالي
PATH	قائمة بالأدلة (مفصولة بنقطتين متعامدتين) والتي ستقوم قشرة نظام التشغيل بالبحث فيها عند البحث عن أحد التطبيقات

ويختلف المتغير (PATH) عن متغيرات البيئة الأخرى التي ناقشناها. وبدلاً من استخدام المتغير (PATH) بوصفه جزءاً من أحد الأوامر، فإن قيمة هذا المتغير تُستخدم مباشرة من قبل قشرة نظام التشغيل (BASH). فعندما يقوم المستخدم بإدخال أمر ما، مثلاً إدخال فايرفوكس (firefox) لبدء متصفح الشبكة، فإن قشرة نظام التشغيل (BASH) تبحث عن هذا الأمر في كل دليل مُدرج في (PATH) على التوالي. وبإمكانك استخدام أمر (which) لمعرفة كيفية القيام بهذا البحث عملياً:

```
[alice@sunshine ~]$ which firefox
/usr/bin/firefox
[alice@sunshine ~]$ which ThisProgramDoesNotExist
/usr/bin/which: no ThisProgramDoesNotExist in (/usr/lib/qt-
3.3/bin:/usr/local/bin:/usr/bin:/bin:/usr/local/sbin:/usr/sbin:/sbin:/
home/alice/bin)
```

المتغيرات المدمجة:

بالإضافــة إلى متغــيرات البيئة، تحتوي قشرة نظام التشــغيل (BASH) على العديد من المتغــيرات المفيدة. وهذه المتغيرات مجتمعة تُدعى بالمتغيرات المدمجة. وتُقدم المتغيرات المدمجة مجموعة واســعة من الوظائف الصغيرة بدءاً من الإفادة بنوع جهاز الخادم الذي يعمل ووصولاً لاســتعادة آخر الأوامر صدوراً. وهناك العشرات من المتغيرات المدمجة التي يمكننا الاختيار من بينها (انظر دليل قشرة نظام التشــغيل للحصول على قائمة كاملة)، لكن سوف نعمل في هذا الكتاب على مجموعة صغيرة من تلك المتغيرات (الجدول ١٠-٣).

ويوضح النص البرمجي في القائمة (٥) مثالاً على كيفية استخدام هذه المتغيرات.

قائمة ٥: (opt/book/scripting/builtin_variable_example):

```
#! /bin/bash
echo «This script is executing with process ID: $$»
echo «OS: $OSTYPE Hardware: $MACHTYPE»
echo «This is he current date and time:»
date
echo «The exit value from date was $?»
echo «This command should fail:»
ls -l NoFile
echo «The exit value was $?»
echo «Wait 2 seconds»
sleep 2
echo «Here are 3 random numbers:»
echo $RANDOM
echo $RANDOM
echo $RANDOM
echo «Wait 3 seconds»
sleep 3
echo «This script has run for $SECONDS seconds»
```

```
[alice@sunshine ~]$ /opt/book/scripting/builtin_variable_example
This script is executing with process ID: 10380
OS: linux-gnu Hardware: i386-redhat-linux-gnu
This is the current date and time:
Wed Dec 19 11:41:40 EST 2012
The exit value from date was 0
This command should fail:
ls: cannot access NoFile: No such file or directory
The exit value was 2
Wait 2 seconds
Here are 3 random numbers:
10549
319
20535
Wait 3 seconds
This script has run for 5 seconds
```

المتغير	الوصف
$?	اســتعادة حالة الخــروج لآخر الأوامر. وقيمة الصفــر (٠) تعني النجاح، في حين تشير أي قيمة أخرى إلى وجود خطأ. وكل قيمة لها معنى مرتبط بتطبيق محدد.
$$	استعادة الرقم التعريفي للنص البرمجي الذي يعمل حالياً.
$MACHTYPE	استعادة هيكلة الجهاز المستخدم.
$OSTYPE	استعادة نظام التشغيل المستخدم.
$SECONDS	استعادة الفترة الزمنية بالثواني والذي عمل خلالها النص البرمجي الحالي.
$RANDOM	استعادة رقم عشوائي بين (٠) و (٣٢٧٦٧).

الجمل الشرطية:

استعرضنا في القسم السابق متغير?$ ووضحنا استعادة قيمة الخروج من آخر الأوامر التي تم تشغيلها. ماذا لو كنت تريد أن تأخذ إجراء معيناً في حال نجاح الأمر (?$ يساوي ٠) وتريد أن تأخذ إجراء آخر في حال فشـله؟ ومثل أي لغة برمجة أخرى فإن قشرة نظام التشـغيل (BASH) توفر تركيبات بإمكانها اختبار مجموعة من الشروط المعينة ومن ثم التصرف بناء على نتيجة الاختبار.

الجملة الشرطية (If/then):

أبسط شكل من أشكال الجمل الشرطية هو شكل (if/then). ويقوم الأمر (if) بفحص قيمة الخروج لسلسـة من تعبـيرات المقارنة. فإذا كانت قيمة الخروج تسـاوي صفراً فإن الأوامر في مقطع (then) يتم تنفيذها. ويمكن إنهاء التركيب بالكامل بواسطة الأمر (fi).

```
#! /bin/bash
if [ «$USER» = «alice» ]
then
    echo «Good Morning, Alice!»
fi
```

وإذا كان المسـتخدم الذي يُشـغل هذا النص البرمجي يحمل اسـم المسـتخدم (alice) («$USER» = «alice») فإنه يتم تنفيذ الأمر (echo). أما إذا كان اسم المستخدم شيئاً آخر فإن النص البرمجي ينتهي دون تنفيذ أي أمر.

إن بناء الجملة الشرطية (if/then) في قشرة نظام التشـغيل (BASH) يختلف نسـبياً عن بناء الجمل الشرطية في معظم لغات البرمجة[٣]. والخطأ الأكثر شيوعاً عند كتابة جملة

---

(٣) قشرة نظام التشغيل (BASH) تدعم تركيبات متعددة لجملة (if/then). انظر الرابط التالي لمزيد من المعلومات:
http://tldp.org/LDP/abs/html/testconstructs.html

(if/then) في قشرة نظام التشغيل (BASH) هو عدم فصل العناصر بمسافات. يجب وضع مســافة بين (if) والأقواس المربعة، كما يجب وضع مسافة في عبارة المقارنة داخل الأقواس. ونجد أن العديد من لغات البرمجة الأخرى أكثر تسامحاً في استخدام المسافة. وفي حال عدم وضع مسافة في جملة (if) فإن العبارة ستفشل ويؤدي ذلك إلى خطأ.

```
if[»$USER» = «alice»]

if [»$USER» = «alice»]

if[ «$USER» = «alice» ]
```

وثمة فرق آخر في استخدام الجملة الشرطية (if/then) في قشرة نظام التشغيل (BASH) مقارنة باللغات البرمجية الأخرى وهذا الفرق هو أن مقارنة العبارات النصية تستخدم عامل مقارنة مختلف (=) عن العامل المســتخدم في المقارنــة العددية (-eq) كما في المثال أعلاه. والجدول التالي يوضح قائمة بعوامل المقارنة مع أمثلة على استخداماتها.

العامل	المقارنة	مثال على الاستخدام
لأمثلة الاستخدام: X = 5 «Y = «RED		
-eq	مساوٍ لـ (عدد صحيح)	if [$X -eq 5]
-ne	غير مساوٍ لـ (عدد صحيح)	if [$X -ne 3]
-gt	أكبر من (عدد صحيح)	if [$X -gt 2]
-lt	أصغر من (عدد صحيح)	if [$X -lt 10]
-ge	أكبر من أو يساوي (عدد صحيح)	if [$X -ge 4]
-le	أصغر من أو يساوي (عدد صحيح)	if [$X -le 7]
=	مساوٍ لـ (نص)	if [«$Y» = «RED»]
!=	غير مساوٍ لـ (نص)	if [«$Y» != «BLUE»]

الجملة الشرطية (If/then/else):

في حـــال كنت تريد أن تتخذ إجراء معينـــاً إذا كانت العبارة الشرطية صحيحة وتريد أن تتخــذ إجراء آخر إذا كانت العبارة الشرطية خاطئة، فإن عليك اســتخدام جملة (If/then/else). وهــذه الجملة مطابقة لجملة (If/then) باســتثناء الأمــر الإضافي في مقطع (else) والذي سيتم تنفيذه عند عدم استيفاء الشرط. وتوضح القائمة (٦) (opt/book/scripting/number_guess_v1) أدناه مثال أساسي على جملة (If/then/else). وسوف نقوم بالبناء على هذا المثال الأساسي لتطوير تطبيقات أكثر تعقيداً في بقية هذا الفصل.

قائمة ٦: (opt/book/scripting/number_guess_v1):

```
#! /bin/bash
guess=2
number=$(( ( $RANDOM % 100) + 1 ))
#Is the guess correct?
if [ $guess -eq $number ]
then
    echo «Correct Guess: The number is $number»
else
     # Is the guess high?
     if [ $number -lt $guess ]
then
     echo «Guess lower: The number is less than $guess»
fi
    # Is the guess low?
if [ $number -gt $guess ]
then
    echo «Guess higher: The number is greater than $guess»
fi
fi
```

ولأن (guess) تساوي ٢ في حين أن الرقم يساوي ٥ فإن الجزء الأول من جملة (if/then) سيكون دائماً خاطئاً (سوف نقوم بوضع تخمينات يمكن إضافتها من المستخدم لاحقاً في هذا الفصــل)، وبناء على ذلك فإن الجزء الموجود في مقطــع (else) يتم دائماً تنفيذه. وفي هذه المرحلة يقوم النص البرمجي بتنفيذ شيء لم نره سابقاً: الجملة الشرطية المتداخلة.

والجملة الشرطية المتداخلة هي جملة (if/then) عادية بداخل جملة (if) أو جملة (else).

```
if [ condition1 ]
then
  echo «condition1 is true»
else
  #Nested-if statement
if [ condition2 ]
  then
     echo «condition2 is true»
   else
     echo «Neither condition is true»
   fi
fi
```

إذا كان الشرط الأول صحيحاً فإن جزء (else) يتم تخطيه. والجملة الشرطية المتداخلة لا يتم تنفيذها أبداً حيث لا يتم تشغيل أي اختبار على الشرط الثاني. لكن إذا لم يكن الشرط الأول صحيحاً فإن الجملة الشرطية المتداخلة يتم تنفيذها كما يتم اختبار الشرط الثاني. وفي النص البرمجي الخاص بتخمين الرقم أعلاه، نجد أن (guess) أقل من ٥ لذا فإن الجزء الأول والثــاني من الجملة الشرطية المتداخلة يعــدّان صحيحين، ومن ثم يُعرض (:Guess higher The number is greater than 2). ويمكننا تشغيل النص البرمجي لاختبار المخرجات:

```
[alice@sunshine ~]$ /opt/book/scripting/number_guess_v1
Guess higher: The number is greater than 2
```

الجملة الشرطية (if/then/elif):

الجملة الشرطية التي سنناقشــها هي جملة (if/then/elif). وهذه الجملة هي صورة مختــصرة لجملــة (else if) كما أنها بديل للجملة الشرطيــة المتداخلة. ويمكن كتابة المثال أعلاه باستخدام هذه الجملة الشرطية كما يلي:

```
if [ condition1 ]
then
  echo «condition1 is true»
elif [ condition2 ]
then
    echo «condition2 is true»
else
    echo «neither condition is true»
fi
```

كــما يمكن إضافة مقاطــع (elif) متعددة لجملة (if) في حــال اختبار أكثر من شرطين. ومثالاً على ذلك سنقوم بتحديث النص البرمجي لتخمين الأرقام كما يلي:

قائمة (7): (opt/book/scripting/number_guess_v2):

```
#! /bin/bash
guess=2
number=$(( ( $RANDOM % 100 ) + 1 ))
#Is the guess correct?
if [ $guess -eq $number ]
then
   echo «Correct guess: The number is $number»
# Is the guess high?
elif [ $number -lt $guess ]
then
echo «Guess lower: The number is less than $guess»
# Is the guess low?
elif [ $number -gt $guess ]
then
echo «Guess higher: The number is greater than $guess»
fi
```

إن استخدام (elif) بدلاً من الجملة الشرطية المتداخلة يجعل التعليمات البرمجية أقصر قليلاً كما يجعلها أسـهل في القراءة. ويمكننا تشـغيل التعليمات البرمجيـة للتأكد من أنها ستؤدي إلى النتائج السابقة نفسها.

```
[alice@sunshine ~]$ /opt/book/scripting/number_guess_v2
Guess higher: The number is greater than 2
```

مدخلات المستخدم:

إن قِيم جميع المتغيرات في النصوص البرمجية التي ناقشناها إلى الآن تُعد ضمنية ومثبتة حيث تــم تحديدها في النص البرمجي، ومن ثم فإن الطريقة الوحيدة لتغيير قيم المتغيرات هــي من خلال تغيير النص البرمجــي. وذلك ملائم في كثير من الحالات، لكن قد نحتاج إلى قيــم يتم إدخالها من قبل المســتخدم. وهناك طريقتان لقبول المدخلات من المســتخدم: معاملات سطر الأوامر، وأمر القراءة (read).

معاملات سطر الأوامر:

وبشــكل مشابه للأوامر التي قمت بتنفيذها في النوافذ الطرفية، فإن النصوص البرمجية لقــشرة نظام التشــغيل (BASH) يمكنها قبول معاملات البرامــج. ويتم تخزين المعاملات بشكل آلي في متغيرات خاصة عند تنفيذ البرامج. ويتم تسمية هذه المتغيرات بأرقام حسب الترتيب الذي حصلت عليه المعاملات في سطر الأوامر:

قائمة (٨): (opt/book/scripting/user_input_ex1):

```
#! /bin/bash
echo «The first argument: $1»
echo «The second argument: $2»
echo «The third argument: $3»

[alice@sunshine ~]$ /opt/book/scripting/user_input_ex1 42 «Hello World»
Earth
The first argument: 42
The second argument: Hello World
The third argument: Earth
```

لاحظ أن المعامل الثاني يتكون من كلمتين («Hello World») حيث إن علامات الاقتباس حول مجموعة من الكلمات تُخبر قشرة نظام التشــغيل (BASH) بأن هذه الكلمات عبارة عن معامل واحد.

إذاً يمكنــا الآن قبول معاملات من ســطر الأوامر، لكن كيف يمكنــا التأكد من إدخال العــدد الصحيح من المعاملات؟ تتضمن قشرة نظام التشــغيل (BASH) متغير خاص وهو ($#) والــذي يقوم بحفظ مجموع عدد المعاملات المدخلة. وهذا المتغير يســمح باختبار عدد المعاملات المدخلة في مقابل عدد المعاملات المتوقع إدخالها ومن ثم طباعة رسالة خطأ عند فشل هذا الاختبار.

قائمة (٩): (opt/book/scripting/user_input_ex2)

```
#! /bin/bash
if [ $# -eq 3 ]
then
echo «The first argument: $1»
echo «The second argument: $2»
echo «The third argument: $3»
else
   echo «Three arguments are required!»
fi
[alice@sunshine ~]$ /opt/book/scripting/user_input_ex2 42 Earth
Three arguments are required!
```

قراءة مدخلات المستخدم:

الخيــار الآخر لأخذ مدخلات المســتخدم بالاعتبار هو أمــر (read) والذي يقوم بإيقاف تنفيذ النص البرمجي حتى يقوم المستخدم بإدخال قيمة ما، ومن ثم يضغط على زر الإرجاع. ولتوضيح استخدام الأمر (read)، سنقوم بتحديث النصي البرمجي لتخمين الأرقام:

قائمة (١٠): (opt/book/scripting/number_guess_v3):

```
#! /bin/bash
#Prompt for user input
echo «Enter a number between 1 and 100 and press [ENTER]: »
read guess

number=$(( ( $RANDOM % 100 ) + 1 ))
#Is the guess correct?
if [ $guess -eq $number ]
then
    echo «Correct guess: The number is $number»
# Is the guess high?
elif [ $number -lt $guess ]
then
echo «Guess lower: The number is less than $guess»
# Is the guess low?
elif [ $number -gt $guess ]
then
echo «Guess higher: The number is greater than $guess»
fi

[alice@sunshine ~]$ /opt/book/scripting/number_guess_v3
Enter a number between 1 and 100 and press [ENTER]: 15
Guess lower: The number is less than 15
```

الحلقات:

أحد أكثر الجوانب فائدة في البرمجة النصية لقشرة نظام التشغيل (BASH) (وفي برمجة الحاسب الآلي بشكل عام) هو القدرة على تخفيض المهام المتكررة إلى عدد بسيط من الأوامر. وبدلاً من كتابة الأوامر المتشابهة نفسها مراراً وتكراراً، فإن الحلقات تسمح لك بكتابة الأوامر التي ترغب في تنفيذها مرة واحدة وبعد ذلك تترك الأمر لقشرة نظام التشغيل لتكرار تلك الأوامر. وسوف نعمل على نوعين من الحلقات المتاحة في النص البرمجي لقشرة نظام التشغيل (BASH):

- حلقات (for): وهذه الحلقات تقوم بتكرار الأوامر باستخدام قائمة من عناصر المدخلات.
- حلقات (while): وهذه الحلقات تقوم بتكرار الأوامر عندما يكون الشرط المُعطى صحيحاً.
- حلقات (for):

وهذه الحلقات هي الأبسط والأكثر استخداماً في النصوص البرمجية لقشرة نظام التشغيل (BASH). وتقوم حلقة (for) بتكرار عناصر القائمة بحيث يتم تنفيذ أي أمر موجود في الحلقة خلال كل دورة. وعندما تصل قشرة نظام التشغيل (BASH) إلى الكلمة المفتاحية (done) سيقوم بالانتقال إلى بداية الحلقة ويبدأ دورة جديدة. وخلال كل مرور متوالٍ في الحلقة فإن قيمة متغير الحلقة (وهو (var) في المثال التالي) تتغير وفقاً للعنصر الحالي في القائمة. والقائمة التالية مثال مبسط على الحلقات:

قائمة (١١): (opt/book/scripting/for_loop_example)

```
#! /bin/bash
for var in «item1» «item2» «item3»
do
   echo «The current item is $var»
#More commands could be added here
done
```

وعند تشغيل هذا المثال سترى أن قيمة (var$) تتغير مع كل دورة:

```
alice@sunshine ~]$ /opt/book/scripting/for_loop_example1
The current item is item1
The current item is item2
The current item is item3
```

وبالإضافة إلى سرد كل عنصر في سـطر الأوامر، فإنه يمكنك اسـتخدام مخرجات الأوامر كقائمة عناصر للتكرار من جديد.

قائمة (١٢): (opt/book/scripting/for_loop_example2):

```
#! /bin/bash
for word in $(head -3 /opt/book/scripting/words.txt)
do
  echo «Original word: $word»
  echo «All uppercase: $(echo $word | tr '[:lower:]' '[:upper:]')»
done
[alice@sunshine ~]$ /opt/book/scripting/for_loop_example2
Original word: eyes
All uppercase: EYES
Original word: record
All uppercase: RECORD
Original word: explosive
All uppercase: EXPLOSIVE
```

وكــما ترى فإن أول ثلاثة ســطور في ملــف (opt/book/scripting/words.txt) (eyes, record, explosive) استُخدمت بصفة قائمة عناصر للتكرار من جديد. الأمر الأول في الحلقة هــو أمر بســيط وهو عبارة عن الأمر (echo) والذي يقوم بعــرض قيمة (Sword)، أما الأمر الثاني فهو أكثر تعقيداً حيث يُنقل في هذا الأمر قيمة المتغير (Sword) إلى الأمر (tr) ومن ثم تُحوَّل الحروف الصغيرة إلى حروف كبيرة (echo Sword I tr ‹[:lower:]› ‹[:upper:]›) وبعد ذلك تُعرض مخرجات هذا الأمر على الشاشة.

فاصل الحقول الداخلية:

عنــد قراءة مخرجات الأوامــر في حلقات (for)، فإن قشرة نظام التشــغيل (BASH) تحدد الفواصل بين العناصر باستخدام متغير داخلي خاص، وهو ($IFS) والذي يقصد به (internal field separator). ويحتوي المتغير على قائمة من الرموز التي تُستخدم حدوداً للحقول. وعندما يُعثر على أحد تلك الحدود، يُنشَــأ عنصر جديد لحلقات (for). والقيم الافتراضية لمتغير ($IFS) هي رموز المسافات (المسافة، والتبويب، والسطر الجديد)، لكن يمكن تغيير هذه القائمة لتحقق عدة أهداف منها على سبيل المثال تحليل قائمة تستخدم الفواصــل، أو تجاهل إحدى القيم الافتراضية كفاصل والســماح لها بــأن تكون جزءاً من عنصر.

قائمة (١٣): (opt/book/scripting/ifs_example1):

```
!# /bin/bash
for line in $(tail -3 /etc/passwd)
do
   echo $line
done
[alice@sunshine ~]$ /opt/book/scripting/ifs_example1
russell.dacanay:x:1648:100: »Russell
Dacanay
(Staff-Library)»:/home/staff/russell.dacanay:/bin/bash
daniel.saddler:x:1649:100: »Daniel
Saddler
(Staff-Student
Services)»:/home/staff/daniel.saddler:/bin/bash
russell.lavigne:x:1650:100: »Russell
Lavigne
(Staff-Academic
Affairs
VP
Office)»:/home/staff/russell.lavigne:/bin/bash
```

وكما ترى فإن اســتخدام القيم الافتراضية للمتغير (IFS$) أدى إلى تقســيم ســطور الملف (etc/passwd) في منتصف العمود الخامس بسبب المسافة أو المسافات الموجودة في حقل النص. ولتعديل هذا الوضع ســوف نقوم بضبط المتغير (IFS$) ليشــمل فقط رمز السطر الجديد ('n\'$).

قائمة (١٤): (opt/book/scripting/ifs_example2):

```
!# /bin/bash
#Change IFS to the newline character only
IFS=$'\n'
for line in $(tail -3 /etc/passwd)
do
   echo $line
done
[alice@sunshine ~]$ /opt/book/scripting/ifs_example1
russell.dacanay:x:1648:100: »Russell Dacanay (Staff-Library)»: \
/home/staff/russell.dacanay:/bin/bash
daniel.saddler:x:1649:100: »Daniel Saddler (Staff-Student Services)»: \
/home/staff/daniel.saddler:/bin/bash
russell.lavigne:x:1650:100: »Russell Lavigne (Staff-Academic Affairs VP
Office)»: \
/home/staff/russell.lavigne:/bin/bash
```

لاحــظ أن الخــط العكسي المائل (\) في المخرجات أعلاه هو رمز لمتابعة الســطر، والذي يســتخدم في حال كون المخرجات طويلة جداً ولا يمكن عرضها في ســطر واحد. وإذا قمت بتشغيل النص البرمجي في آلة لينكس الافتراضية فإنك ستجد السطر وفيه خط عكسي مائل (\) وستجد ما بعده معروضاً في سطر واحد.

التسلسلات:

غالباً ما تحتاج إلى تنفيذ أمر ما لعدد محدد من المرات، أو تحتاج إلى اســتخدام سلسلة من الأرقام كمدخلات للحلقات. ومنذ الإصدار الثالث[٤] لقشرة نظام التشــغيل (BASH)، احتوت القشرة على قاعدة مدمجة لتوليد سلســلة من الأرقام كمدخلات للحلقات. وتكون سلســلة الأرقام محاطة بأقواس متعرجة ({ })، كما تكون المعاملات مفصولة بنقطتين (..). ويمكن إنشاء السلسلة إما باستخدام معاملين وإما بثلاثة معاملات، فإذا أعطي عاملان، فإن الأول هو متغير البداية والثاني هو متغير النهاية. وبعد ذلك يتم تنفيذ الحلقة باســتخدام جميع الأعداد الصحيحة بدءاً من متغيرة البداية وانتهاءً بمتغيرة النهاية.

قائمة (١٥): (opt/book/scripting/sequence_example1):

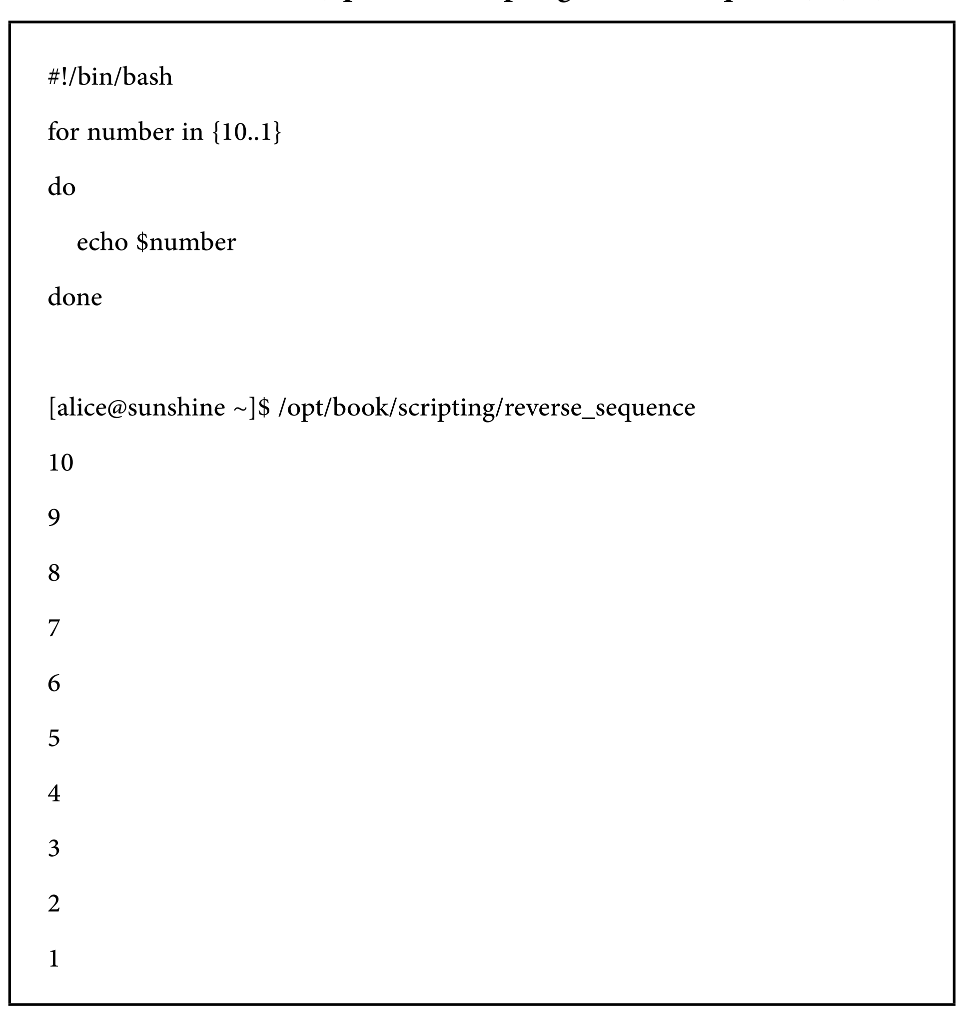
```
#!/bin/bash
for number in {1..5}
do
   echo $number
done

[alice@sunshine ~]$ /opt/book/scripting/sequence_example1
1
2
3
4
5
```

(٤) ولمزيد من المعلومات حول توليد المتسلسلات في الإصدارات السابقة، انظر أمر (seq) في صفحات الدليل.

ويمكنـــك أيضاً إضافة الأرقام عكســـياً من خلال جعل الرقم الأكـــبر قيمة البداية والرقم الأصغر قيمة النهاية.

قائمة (١٦): (opt/book/scripting/reverse_sequence):



```
#!/bin/bash
for number in {10..1}
do
   echo $number
done

[alice@sunshine ~]$ /opt/book/scripting/reverse_sequence
10
9
8
7
6
5
4
3
2
1
```

وإذا تم إعطاء ثلاثة معاملات[٥] فإن المعامل الثالث يحدد مقدار الزيادة بين كل الأرقام في هذه السلسلة.

(٥) يتوجب استخدام الإصدار الرابع من قشرة نظام التشغيل (BASH) أو أعلى.

قائمة (١٧): (opt/book/scripting/sequence_example3):

```
#!/bin/bash
for number in {1..10..2}
do
  echo $number
done

[alice@sunshine ~]$ /opt/book/scripting/sequence_example3
1
3
5
7
9
```

لاحظ أن الرقم (١٠) لم يكن من ضمن النتائج التي تم الحصول عليها، وذلك لأن سلسلة الأرقام تحتوي على جميع الأرقام الأقل من أو يساوي قيمة النهاية. وبما أن السلسلة تزيد بـ (٢) فإن الرقم التالي في السلسلة هو (١١) لكن هذا العدد أكبر من قيمة النهاية وهي (١٠).

التوقف والاستمرار:

قـد ترغب في ظل ظروف معينة في إيقـاف معالجة الحلقة أو قد ترغب في التجاوز إلى الـدورة التالية من الحلقة. الكلمات المفتاحية (break) و(continue) تعطيك القدرة على القيـام بذلك. وتقوم الكلمة المفتاحية (break) بإيقـاف معالجة الحلقة، وتخطي الأوامر المتبقيـة في الدورة الحالية من الحلقة، وتخطي العنـاصر المتبقية في قائمة المدخلات. لكن تنفيذ النص البرمجي لا يتم مقاطعته حيث يستمر في تنفيذ الأوامر بعد الحلقة.

قائمة (١٨): (opt/book/scripting/break_example):

```
#!/bin/bash
for number in {1..5}
do
if [ $number -eq 4 ]
then
  echo «Stop!»
  break
fi
echo «$number»
done
echo «This command runs AFTER the loop is complete.»

[alice@sunshine ~]$ /opt/book/scripting/break_example
1
2
3
Stop!
This command runs AFTER the loop is complete.
```

لاحظ أنه تمت معالجة الحلقة كما هو متوقع وذلك للأرقام الثلاثة الأولى من السلسلة. فعندمـا تم تحقيق الـشرط في جملة (if) ($number –eq4) فقد تم عرض كلمة (Stop!) عـلى الشاشـة، وعندها تم الوصول إلى الكلمـة المفتاحية (break) ومن ثـم ينتهي تنفيذ الحلقة. وفي مثال آخر سـنقوم بتحديث النص البرمجي التابع لتخمين الأرقام وذلك لإعطاء المستخدم خمس فرص لتخمين الرقم ويتوقف إذا تم تخمين الرقم الصحيح.

قائمة (١٩): (opt/book/scripting/number_guess_v4):

```
#! /bin/bash
number=$(( ( $RANDOM % 100 ) + 1 ))
#Give the user 5 guesses
for loop in {1..5}
do
#Prompt for user input
echo «Enter a number between 1 and 100 and press [ENTER]: »
read guess
echo «»
#Is the guess correct?
if [ $guess -eq $number ]
then
    echo «Correct guess: The number is $number»
    echo «You guessed it in $loop tries»
        break
# Is the guess high?
elif [ $number -lt $guess ]
then
    echo «Guess number $loop»
    echo «Guess lower: The number is less than $guess»
# Is the guess low?
elif [ $number -gt $guess ]
then
  echo «Guess number $loop»
  echo «Guess higher: The number is greater than $guess»
fi
end

[alice@sunshine ~]$ /opt/book/scripting/number_guess_v4
Enter a number between 1 and 100 and press [ENTER]: 15

Guess number 1
Guess lower: The number is lower than 15
Enter a number between 1 and 100 and press [ENTER]: 3

Guess number 2
Guess higher: The number is higher than 3
Enter a number between 1 and 100 and press [ENTER]: 5

Correct guess: The number is 5
You guessed it in 3 tries
```

أما الكلمة المفتاحيــة (continue) فتقوم بتجاوز الأوامر المتبقية في الدورة الحالية من الحلقــة وتعمل على بدء دورة جديــدة. وفي المثال التالي سنســتخدم ذات الرمز البرمجي لقائمة (١٨) لكن سنقوم باستخدام الكلمة المفتاحية (continue) بدلاً من الكلمة المفتاحية (break).

قائمة (٢٠): (opt/book/scripting/continue_example):

```
#!/bin/bash
for number in {1..5}
do
if [ $number -eq 4 ]
then
      echo «Stop!»
      continue
fi
echo «$number»
done

echo «This command runs AFTER the loop is complete.»

[alice@sunshine ~]$ /opt/book/scripting/continue_example
1
2
3
Stop!
5
```

ويعمل هذا الأمر بعد اكتمال الحلقة.

لاحــظ الفرق بين مخرجات هذا النص البرمجي وبــين مخرجات النص البرمجي في قائمة (١٨). تمــت معالجة دورات الثـلاث الأولى مرة أخرى كما هو متوقع، كما تم تحقيق شرط جملــة (if) في الدورة الرابعة. لكن وبدلاً من الخروج من الحلقة، تم الاســتمرار في الدورة الخامسة (والأخيرة) من الحلقة.

حلقات (while):

بــدلاً مــن العمل على قائمة مــن العناصر كما هو الحال في حلقــات (for) فإن حلقات (while) تســتمر في العمل حتى يتم تحقيــق شرط معين. وقبل البدء في دورة الحلقة يتم اختبــار الشرط. فإذا كان الشرط صحيحاً فإنه يتم تنفيذ الأوامر داخل الحلقة. أما إذا كان خاطئاً فإنه يتم تجاوز الحلقة، ويتم تنفيذ ما تبقى من النص البرمجي.

قائمة (٢١): (opt/book/scripting/while_loop_example1):

```
#! /bin/bash
counter=1
while [ $counter -le 5 ]
do
   echo $counter
   $(( counter=$counter + 1 ))
done

[alice@sunshine ~]$ /opt/book/scripting/while_loop_example1
1
2
3
4
5
```

وكما ترى فإن مخرجات هذا الأمر مشابهة لمخرجات بعض أمثلة الحلقات التي عرضناها ســابقاً. لكن هناك اختلافات رئيسية في النص البرمجي نفسه. الفرق الأول الذي ستُلاحظه أنه وعلى عكس اســتخدام حلقــات (for) فقد قمنا بتحديد القيمــة الأولية لمتغير العداد (counter) قبل تنفيذ الحلقة.

عندمـا تصل قـشرة نظام التشـغيل (Bash) إلى جملة (while)، يتـم اختبار القيمة الحالية للعداد. فإذا كانت أقل من أو تسـاوي ٥ فإنه يتم تنفيذ الأوامر الموجودة داخل الحلقـة، وعند ذلك يتـم عرض القيمة الحالية للعداد على الشاشـة ومن ثم يتم زيادتها بواحـد (((counter=$counter+1))$) وعند هذه النقطـة يتم اختبار قيمة العداد مرة ثانية وإذا كانت قيمته أقل من أو تساوي ٥ فإن الحلقة تستمر.

وعند كتابة نص برمجي قد تحتاج لإنشاء حلقة لا نهائية، وهي حلقة تستمر حتى يقوم المسـتخدم بإنهائها. وعادة تسـتخدم الحلقة اللانهائية عند الرغبة في مراقبة شيء ما على فترات منتظمة مثل حجم الملف، أو عدد المستخدمين الذين قاموا بتسجيل الدخول. ويمكن إنشـاء الحلقة اللانهائية عن طريق إنشـاء حلقة (while) تكون فيها نتيجة اختبار الشرط دائمـاً صحيحة. وتوضح قائمة (٢٢) مثالاً على اسـتخدام حلقة لا نهائية لمراقبة حجم ملف السـجل (/var/log/httpd/access_log). ومـع كل دورة يتم عرض كل من وقت فحص الملف وحجم ملف السـجل على الشاشة. وسيسـتمر النص البرمجي حتى يقوم المستخدم بالخروج منه إما عن طريق الضغط على مفتاحي (CTRL) و(C) معاً أو عن طريق إغلاق النافذة الطرفية التي يعمل فيها النص البرمجي.

قائمة (٢٢): (opt/book/scripting/while_loop_example2):

```
#! /bin/bash
echo «This script will loop forever.  Hit Control+C (CTRL+C) to exit.»
while [ true ]
do
   sleep 2
   echo «»
   date
   echo «$(wc -l /var/log/httpd/access_log)»
done

[alice@sunshine~]$ /opt/book/scripting/while_loop_example2
This script will loop forever.  Hit Control+C (CTRL+C) to exit.

Fri Jan 4 08:11:00 EST 2013
 7 /var/log/httpd/access_log

Fri Jan 4 08:11:02 EST 2013
 7 /var/log/httpd/access_log

Fri Jan 4 08:11:04 EST 2013
 8 /var/log/httpd/access_log

Fri Jan 4 08:11:06 EST 2013
 9 /var/log/httpd/access_log
```

ويمكــن اختبار هــذا النص البرمجــي وذلك بزيــارة الموقع الإلكــتروني (http://www.sunshine.edu) وذلك بعد تشغيل النص البرمجي. وستلاحظ أن عدد الإدخالات في ملف السجل يزداد في كل مرة تقوم فيها بتحميل صفحة الشبكة.

نظرة عامة لما سبق:

لقد اســتعرضنا فيما سبق الأجزاء الأساســية للنص البرمجي لقشرة نظام التشغيل. الآن نستعرض نص برمجي يستخدم العديد من تلك الأجزاء وذلك لأتمتة إحدى العمليات لجميع مســتخدمي النظام. وتحتوي آلة لينكس الافتراضية المســتخدمة في هذا الكتاب على أكثر من ١٠٠٠ حســاب والتي تُعد كثيرة جداً ويصعب دعمها يدوياً. ويقوم هذا النص البرمجي باستخراج المعلومات الهامة لكل حساب كما يقوم بعرضها بشكل يمكن قراءتها بسهولة.

قائمة (٢٣): (opt/book/scripting/user_info):

```
#! /bin/bash
#This script returns import information about all users on the system

#Example line from /etc/passwd
#alice:x:501:501:Alice Adams:/home/alice:/bin/bash
for user in $(cut -d: -f1 /etc/passwd)
do
   IFS=$'\n'
   #Grab the line from the password file that
   #contains this user's info.  We append the
   #delimiter (:) to ensure we only get results
   #for this username and not similar users
   userinfo=$(grep $user: /etc/passwd)

   comment=$(echo $userinfo | cut -d: -f5)
   home=$(echo $userinfo | cut -d: -f6)
   groups=$(groups $user | cut -d: -f2)

  #We only want this to run on «regular» users,
  #not system accounts.  Skip users that do not
  #have '/home' in the path to their home directory
   if [ $(echo «$home» | grep -v '/home/') ]
   then
      continue
   fi

   echo «Username: $user»
   echo «User Info: $comment»
   echo «Home Directory: $home»
   echo «Groups: $groups»

   echo «Disk usage: $(du -sh $home)»

   last=$(last $user | head -1)

   if [ $(echo $last | wc -c) -gt 1 ]
   then
      echo «Last login: »
      echo «$last»
   else
      echo «User has never logged in!»
   fi
   echo «»
   echo «--»
   echo «»
done

[alice@sunshine ~]$ /opt/book/scripting/user_info
Username: alice
User Info: Alice Adams
Home Directory: /home/alice
Groups: alice sys
Disk Usage: 75M /home/alice
Last login:
alice pts/3 sunshine.edu Sun Jan 13 12:22 - 13:00 (0:48)
--
Username: bob
User Info: Bob Brown
Home Directory: /home/bob
Groups: bob
Disk Usage: 1.1M /home/bob
Last login:
bob pts/6 sunshine.edu Sun Jan 6 16:48 - 18:46 (1:58)
```

وبإلقاء نظرة تفصيلية على هذا النص البرمجي، نلاحظ أنه في الســطور الأولى تم تكوين حلقة باســتخدام جميع أسماء المســتخدمين في النظام، إذ إن اسم المستخدم يكون دائماً في العمود الأول من ملف (/etc/password).

```
for user in $(cut -d: -f١ /etc/passwd)
do
```

تــم البحث في ملف (/etc/password) لكل الحســابات وذلــك للعثور على معلومات الحساب لكل مستخدم.

```
IFS=$'\n'
userinfo=$(grep $user: /etc/passwd)
```

أما القســم التالي من النص البرمجي فقد اســتخدم الأمر (cut) لفصل أعمدة معلومات الحسابات إلى متغيرات قابلة للاستخدام. كما استخدم الأمر (groups) للحصول على قائمة المجموعات التي ينتمي إليها المســتخدم. أيضاً تم اســتخدام الأمر (du) لحساب المساحة التخزينية التي يستخدمها الدليل الرئيسي لكل مستخدم.

```
omment=$(echo $userinfo | cut -d: -f٥)
home=$(echo $userinfo | cut -d: -f٦)
groups=$(groups $user | cut -d: -f٢)
echo «Username: $user»
echo «User Info: $comment»
echo «Home Directory: $home»
echo «Groups: $groups»
echo «Disk usage: $(du -sh $home)»
```

وفي الجزء الأخير من النص البرمجي تم استخدام الأمر (last) للحصول على أحدث دخول للمستخدمٍ. وإذا لم يقم المستخدم بتسجيل الدخول مطلقاً، فإن نتيجة أمر (last) ستكون سطراً فارغاً، كما سيعرض النص البرمجي رسالة بحدوث خطأ. أما إذا قام المستخدم بتسجيل الدخول فإنه يُعرَض آخر تسجيل دخول للمستخدم ومدة تسجيل الدخول.

```
last=$(last $user | head -1)
if [ $(echo $last | wc -c) -gt 1 ]
then
  echo «Last login:»
  echo $last
else
  echo «User has never logged in!»
fi
```

نموذج حالة-ماكس بتلر (Max Butler):

في عـــام ١٩٩٨ كان ماكس بتلــر (Max Butler)، والذي يبلغ من العمر ٢٦ عاماً آنذاك، أحد المتحمســين للحاســب الآلي ويكسب أكثر من ١٠٠ دولار في الســاعة من خلال اختبار أمــن الــشركات التي يتعامل معها، كــما كان أحد المتطوعين في مكتــب التحقيق الفيدرالي بســان فرانسيســكو. وفي تلك السنة تم اكتشــاف ثغرة أمنية حرجة في معظم خوادم اسم المجال (DNS) الشائعة الاستخدام على الإنترنت والمفتوحة المصدر والمعروفة بـ (BIND). ويُســتخدم (BIND) فعلياً على جميع الخــوادم وذلك لربط عناويــن المواقع الإلكترونية (URLS) مثــل (www.usf.edu) بعناويــن بروتوكــول الإنترنــت (IP addresses) مثــل (١٣١,٢٤٧,٨٨,٨٠). وتســمح تلك الثغرة المُكتشفة لقراصنة الحاسب بالحصول على تحكم كامــل لأي خادم يقوم بتشــغيل إصدار غير محمي مــن (BIND). وبالتحديد فإن جميع خــوادم وزارة الدفاع الأمريكية تعمل على (BIND). ولحماية هذه الخوادم من المهاجمين لابد من القيام بعمليات التصحيح المطلوبة قبل أن يصل المهاجمون إليها. لكن البيروقراطية العســكرية بطيئة نوعاً ما. كيف لخبير أمني مهتم بهذا الموضوع، مع ما يحمله من براءة شاب ذي عشرين عاماً، أن يصلح هذا الخلل في أسرع وقت ممكن؟

الدخول للبرمجة النصية. النص البرمجي يمكنه العمل بنفس سرعة جهاز الحاسب الآلي، كما يمكنــه توجيه المئات من أجهزة الحاســب الآلي في كل ثانية لتحميل تصحيح معين ومن ثم

قيام الأجهزة بإصلاح نفسها. ماكس بتلر (Max Butler) قام بفعل ذلك حيث قام بتجهيز نص برمجي يســتطيع العثــور على أي خادم يعمل على إصدار غــير محدث من (BIND) ومــن ثم تحديــث هذا الإصدار بالتصحيح المحدد. وفي أثنــاء ذلك، قام ماكس بتلر (Max Butler) بتعديل التصحيح بحيث ينشــئ باباً خفياً لا أحد يعلم عنه. ويعتقد ماكس بهذه الطريقــة أنه يحمي أجهزة الحاســب الآلي من المهاجمين، في حــين أنه في الوقت ذاته يُتيح لنفســه الوصول غير المقيد لنفس أجهزة الحاسب الآلي حتى يتمكن من الدخول وإصلاحها في المرة القادمة التي يتم فيها الإبلاغ عن ثغرة ما. وبناء على ذلك لا حاجة لإضاعة الوقت في التواصل مع مسؤولي وزارة الدفاع.

وهذا العمل تم بشــكل جيد لكن ولسوء حظ ماكس فإن الباب الخفي لم يُعد عملاً حسناً. فعندما علم مسؤولو وزارة الدفاع عن الباب الخفي، قاموا بمحاكمة ماكس. وفي يوم ٢١ من شهر مايو من عام ٢٠٠١ أُرسل ماكس إلى السجن لمدة ١٨ شهراً بسبب هذا العمل.

وهــذه لم تكن الحالة الأخيرة لماكس مع جرائم الإنترنت أو الســجن. ففي وقت لاحق قام ماكس بقيادة غالبية ســوق بطاقات الائتمان غير المشروعة. وفي الثاني عشر من شهر فبراير مــن عــام ٢٠١٠ تم الحكم على ماكس بالســجن لمدة ١٣ عاماً لهــذه الجريمة، وهي أطول مدة تم الحكم فيها في جرائم الحاسب الآلي. لكن هذه الحالة جرى التفوق عليها من قبل الحكــم الصادر عــلى ألبرت غونزاليــس (Albert Gonzales) في قضية تي جي ماكس (TJ. Maxx). وحاليــاً يقــضي ماكس عقوبته في ســجن (Yankton Federal Prison Camp)، ويتصف هذا الســجن بالحــد الأدنى من الأمن في ولاية جنوب داكوتــا (South Dakota). ومن المقرر أن يُفرج عنه في الأول من يناير من عام ٢٠١٩. وقد أنتجت محطة (CNBC) التلفزيونية ملفاً عن هذه الحالة باسم «الجشع الأمريكي» (American greed).

المراجع:

http://www.wired.com/techbiz/people/magazine/17-01/ff_max_butler?currentPage=all

Poulsen, K. «Kingpin: how one hacker took over the billion-dollar cybercrime underground,» Random House.

http://www.cnbc.com/id/100000049

الملخص:

استـــعرض هذا الفصل النصوص البرمجية لقشرة نظام التشـــغيل وفوائدها. فالنصوص البرمجية تُعد واحدة من أقوى الأدوات في ترســـانة متخصــصي تقنية المعلومات، وخصوصاً متخصــصي أمن المعلومات. ويســـتطيع المتخصص أن يجمع كل خبرتــه المهنية في مخزون النصوص البرمجية، وذلك لإعادة استخدامها في اللحظة المناسبة. ولقد حاولنا في هذا الفصل اســـتخدام حالات مثيرة للاهتمام وذلك لتقديم هذا الموضوع، ونأمل أن تكون مصدر إلهام لتطوير النصوص البرمجية الخاصة بك لأتمتة المهام المتكررة في عملك اليومي.

وتحتوي مكتبة المطور التابعة لشركة أبل (Apple) على فصل موجز ومكتوب بطريقة جيدة عن البرمجة النصية لقشرة نظام التشغيل وعنوان ذلك الفصل (Shell scripting primer)[٦].

أسئلة مراجعة للفصل:

١. ما البرمجة النصية لقشرة نظام التشغيل؟

٢. فيمَ تُستخدم البرمجة النصية لقشرة نظام التشغيل؟ وما فائدة هذا الاستخدام؟

٣. ما الفرق المهم بين لغات البرمجة النصية ولغات الحاسب الآلي الأخرى؟

٤. ما السطر الأول في النص البرمجي لقشرة نظام التشغيل (BASH)؟

٥. ما الذي يحدث إذا لم يملك ملف النص البرمجي أذونات التنفيذ وذلك للمســـتخدم الذي يحاول تشغيل النص البرمجي؟

٦. ما إعادة توجيه المخرجات؟ وما فائدته؟

٧. ما الرمز الذي يعيد توجيه مخرجات أحد الأوامر ليكون مدخلاً لأمر آخر؟

٨. كيف يمكن إرسال مخرجات النص البرمجي إلى ملف ما؟ وما فائدة ذلك؟

٩. هل يؤدي الأمران التاليان: (echo «$PATH»)، و(echo «$PATH») إلى المخرجات نفسها؟

---

(6) http://developer.apple.com/library/mac/#documentation/OpenSource/Conceptual/ShellScripting/Introduction/Introduction.html (accessed 07/19/2013)

١٠. ما الرمز الذي تستخدمه قشرة نظام التشغيل (BASH) لتمثيل الضرب الحسابي؟

١١. مـا الرمز المُسـتخدم لبدء الملاحظـات في النـص البرمجي لقشرة نظام التشـغيل (BASH)؟

١٢. ما الذي يقوم به الأمر (cut)؟

١٣. فيم يُستخدم الأمر (sort)؟

١٤. فيم يُستخدم الأمر (uniq)؟

١٥. في العبارات التالية التي تحدد قيمة المتغير، أي منها يُعتبر صحيحاً؟

- (myVariable = 35)
- (myVariable = 35)
- (myVariable= 35)
- (myVariable =35)

١٦. ما الرمز الذي يقرأ البيانات من الملف ويستخدمها كمُدخل لأمر آخر؟

١٧. ما متغيرات البيئة؟ وما فائدتها؟

١٨. ما المتغيرات المدمجة؟ وما الفرق بينها وبين متغيرات البيئة؟

١٩. ما القيمة المُفترضة لـ (?$) إذا تم تنفيذ آخر أمر بنجاح؟

٢٠. كيف يمكن جمع مُدخلات المُستخدم من النص البرمجي؟

٢١. عند العمل على معاملات سـطر الأوامر، ما المتغير الذي سـيؤدي إلى المعامل الثاني (second argument)؟

٢٢. مـا فاصل الحقل الداخلي؟ وما قيمتـه الافتراضية؟ وكيف يمكن تغيير تلك القيمة الافتراضية؟ ولماذا نقوم بتغيير القيمة الافتراضية؟

٢٣. ما سلسلة الأرقام الناتجة عن {١..١٠..٣}؟

٢٤. ما الحلقات؟ وما فائدتها؟

٢٥. متى تنتهي حلقة (while)؟

أسئلة على نموذج الحالة:

١. ما هي بعض المؤسسات التي تأثرت بالنص البرمجي لـ ماكس بتلر (Max Butler)؟

٢. يدّعي ماكس بتلر (Max Butler) أنه قام بتثبيت الباب الخفي في أجهزة الحاسب الآلي المُصابة بنية حسنة وذلك حتى يتمكن من إصلاح الأجهزة بنفسه في المستقبل. كيف ترد على هذا الادعاء. وبمعنى آخر، إلى أي مدى تعتقد أن هذا الادعاء يعفيه من الذنب؟

نشاط التدريب العملي - أساسيات البرمجة النصية:

تهدف هذه الأنشطة لتطبيق المعارف المكتسبة من هذا الفصل والمتعلقة بأوامر وآليات البرمجة النصية. باستخدام آلة لينكس الافتراضية التي قمت بتثبيتها في الفصل الثاني من هذا الكتاب، افتح نافذة طرفية عن طريق اختيار لوحة أدوات النظام (System Tools) تحت قائمة التطبيقات (Applications). وبعد الانتهاء من كل خطوة، قم بإرسال صورة من شاشة المخرجات إلى أستاذ المادة.

١. احفظ مخرجات الملف (opt/book/scripting/user_info) في ملف نصي، وأعط هذا الملف الجديد الاسم التالي (opt/book/scripting/results/exercise1)

٢. اكتب نصاً برمجياً، وأعطه الاسم التالي (/opt/book/scripting/results exercise2)، حيث يقوم هذا النص البرمجي بما يلي:

- ذكر جميع الملفات في دليل (/usr/bin) والتي يحتوي اسمها على كلمة (my).
- حفظ قائمة الملفات السابقة في ملف (/tmp/exercise1.txt).
- عرض عدد الملفات التي تم العثور عليها للمستخدم.

٣. اكتــب نصــاً برمجيــاً، وأعطــه الاســم التــالي (/opt/book/scripting/results/exercise3)، حيث يقوم هذا النص البرمجي بما يلي:

- سؤال المستخدم عن طول وعرض غرفة مستطيلة الشكل (بالقدم).
- حساب مساحة الغرفة.
- عرض النتيجة للمستخدم.

٤. اكتــب نصــاً برمجيــاً، وأعطــه الاســم التــالي (/opt/book/scripting/results/exercise4)، حيث يقوم هذا النص البرمجي بما يلي:

- العد العكسي من ١٠ إلى ١.
- عرض الرقم الحالي.
- التوقف لثانية واحدة بين الأرقام.
- عرض النص التالي (LFIT OFF) بعد الوصول إلى الرقم ١.

٥. اعمل نسخة لملف (opt/book/scripting/while_loop_example1) وأعطها الاسم التالي (opt/book/scripting/results/exercise٥) وقم بإجراء التعديلات التالية:

- اطلب من المستخدم إدخال الرقم الأعلى.
- اعرض جميع الأرقام الزوجية انتهاءً بالعدد الأعلى.

٦. اعمل نســخة لملف (opt/book/scripting/number_guess_v4) وأعطها الاسم التــالي (opt/book/scripting/results/exercise6) وقــم بتحديث الملف بحيث يعطي المستخدم العديد من الفرص اللازمة لتخمين الرقم.

٧. اعمل نسخة لملف (opt/book/scripting/user_info) وأعطها الاسم التالي (/opt/book/scripting/results/exercise٧) وقم بتحديث الملف بحيث:

- يقبل اسم المستخدم كمعامل لسطر الأوامر.
- بدلاً من عرض معلومات جميع الحسابات، يقوم بعرض مخرجات هذا الحساب فقط.

النتائج المطلوب تسليمها: قم بتسليم جميع الملفات في دليل (/opt/book/scripting/results) إلى أستاذ المادة.

تمرين التفكير النقدي - أمن النص البرمجي:

- تُعد البرمجــة النصية ذات فائدة كبيرة. لكن في كتاب متخصص في أمن المعلومات سنكون مقصرين إذا لم نلفت انتباه القارئ إلى المخاوف الأمنية الهامة ذات العلاقة بالبرمجــة النصية. وتحتــوي صفحات المطــور التابعة لشركة أبــل (Apple) على معلومات عن أمن البرمجة النصية لقشرة نظام التشغيل والتي من أهمها ما يلي:
- إذا لم يتــم تحديد مســارات الأوامر كاملة، فإن النص البرمجي قد ينتهي بتشــغيل تعليمات برمجية ضارة لها اسم الأمر نفسه الذي يتم تنفيذه من قبل النص البرمجي.
- في حــال قبول مدخلات المســتخدم دون تحقق، فإن المســتخدم المُطّلع يســتطيع استغلال امتيازات النص البرمجي. لذلك فإن مدخلات المستخدم يجب أن تُستخدم فقــط في أضيق الحــدود بحيث تتطابق تلــك المدخلات مع مجموعــة من القيم المسموح بها.
- لا ينبغي للنصوص البرمجية أن تحدد ما إذا كان لدى المستخدم الامتيازات المطلوبة لتنفيــذ النص البرمجي. فالمســتخدم الــذي ينفذ النص البرمجي يســتطيع تعديل متغيرات البيئة لإحباط تلك الفحوصات.

المراجع:

Apple Corp., «Shell scripting primer,» http://developer.apple.com/library/mac/#documentation/OpenSource/Conceptual/ShellScripting/ShellScriptSecurity/ShellScriptSecurity.html#//apple_ref/doc/uid/TP40004268-CH8-SW1 (accessed 072013/19/)

أسئلة على البرمجة النصية لقشرة نظام التشغيل:

١. إذا كانــت النصــوص البرمجية تُســتخدم في المقام الأول من قبل مســؤولي النظام أصحاب الخبرة، فلماذا يجب أن نهتم بأمن النصوص البرمجية؟

٢.   لماذا يُعد تنفيذ النصوص البرمجية من قبل مستخدم «جذر» (root user) أمراً خطيراً؟

تصميم حالة:

تم اســتدعاؤك للتحقيق في خــرق محتمل في صنــدوق (Ubuntu Linux). وفي هذه الحالــة من المفيد النظر في ملف الســجل الذي يحفظ معلومات تســجيل الدخول (ssh) (وهي خدمة تســجيل الدخول عن بعد لمضيف نظام ينكس). وفيما يلي مقطع من ملف (auth. log). والملــف الكامــل موجود في آلة لينكس الافتراضيــة في الدليل (/opt/book/scripting/desing_cas/auth.log).

```
Feb 17 08:00:08 inigo sshd[7049]: Failed
password for root from
61.136.171.198 port 59146 ssh2
Feb 17 08:00:09 inigo sshd[7049]: Received
disconnect from
61.136.171.198: 11: Bye Bye [preauth]
Feb 17 08:00:16 inigo sshd[7051]: pam_
unix(sshd:auth): authentication
failure; logname= uid=0 euid=0 tty=ssh
ruser= rhost=61.136.171.198
user=root
Feb 17 08:00:18 inigo sshd[7051]: Failed
password for root from
61.136.171.198 port 59877 ssh2
Feb 17 08:00:19 inigo sshd[7051]:
Connection closed by 61.136.171.198
[preauth]
Feb 17 08:17:01 inigo CRON[7296]: pam_
unix(cron:session): session
opened for user root by (uid=0)
Feb 17 08:17:01 inigo CRON[7296]: pam_
unix(cron:session): session
closed for user root
```

١. قم بإنشاء نص برمجي يستعرض عناوين بروتوكل الإنترنت (IP addresses) (بدون تكرار) لجميع الخوادم التي حاولت الدخول وفشلت في تسجيل الدخول كمستخدم «جذر»، كما يستعرض النص البرمجي عدد المرات التي حاول فيها كل خادم تسجيل الدخول. وقم بفرز النتائج وفقاً لعدد مرات تسجيل الدخول الفاشلة.

٢. قم بإنشاء نص برمجي يستعرض جميع أسماء الحسابات التي تم تجريبها ولا وجود لهـا في هذا الخادم (تلميـح: ابحث عن عبـارة (Failed password for invalid user))، كما يسـتعرض النص البرمجي عناوين بروتوكل الإنترنت (IP addresses) التي صدرت منها تلك المحاولات. وقم بفرز النتائج أبجدياً بحيث لا تشمل السطور المكررة.

٣. قم بإنشـاء نص برمجي يقرأ ملف (ip.txt) والذي يحتـوي على قائمة من عناوين بروتوكل الإنترنت (IP addresses) كما يحاول النص البرمجي تحديد «اسـم المجال المؤهل بشكل كامل» (Fully Qualified Domain Name) أو اختصاراً (FQDN) باستخدام الأمر (host). ويُعد (FQDN) مساعد الذاكرة البشري لعناوين بروتوكل الإنترنت مثـل (www.google.com) أو (my.usf.edu). ويجب أن يحفظ النص البرمجي عناوين بروتوكل الإنترنت و «اسم المجال المؤهل بشكل كامل» (FQDN) (وإذا لم يمكن تحديد عنوان بروتوكل الإنترنت يجب أن يحفظ النص البرمجي عبارة «غير معروف» (UNKNOWN)) وذلك في ملف باسـم (fqdn.txt) بحيث تكون كل مجموعة في سطر واحد ويتم الفصل بينهم بفواصل.


٥٧٨

الفصل الحادي عشر

التعامل مع الحوادث الأمنية

نظرة عامة:

في هذا الفصل سنُلخص الحديث عن المفاهيم والأفكار العديدة التي استعرضناها في الفصول السابقة بإحدى الحوادث الأمنية. فالتعامل مع الحوادث الأمنية جانب مهم من جوانب الأمن لأنه ينطوي على التقليل من التأثير السلبي للحادث على الأصول. ويساعد تطبيق الضوابط اللازمة على تقليل تعرض الأصول للتهديدات القائمة، ومن ثم استعادة خدمات تقنية المعلومات بأقل تأثير في المنظمة قدر الإمكان. في نهاية هذا الفصل يجب أن تكون قادراً على:

- تحديد العناصر الرئيسية في التعامل مع الحوادث الأمنية.
- فهم دورة حياة التعامل مع الحوادث الأمنية.
- إعداد سياسة أساسية تضع منهجية للتعامل مع الحوادث الأمنية.
- استخدام المواد التي استعرضناها سابقاً في تحديد وتصنيف الحوادث الأمنية بشكل صحيح.
- تحديد الوقت المناسب لبدء عملية احتواء الحوادث الأمنية والقضاء عليها.
- إعداد تقرير بالحوادث الأمنية وذلك لتحسين الاستعداد المستقبلي للحوادث الأمنية المماثلة.
- معرفة عناصر التعافي من الكوارث والتخطيط لاستمرارية الأعمال.

مقدمة عن الحوادث الأمنية:

وفقاً لإدارة مخاطر تقنية المعلومات (rev2 61-NIST 800) فإن حوادث أمن الحاسب الآلي هي انتهاك أو تهديد وشيك بانتهاك سياسات أمن الحاسب الآلي، أو سياسات الاستخدام المقبول، أو ممارسات الأمان الموحدة. ومن الأمثلة على الحوادث الأمنية ما يلي:

- مهاجم يأمر روبوتات بإرسال عدد كبير من طلبات الاتصال لخادم ويب المنظمة مما يؤدي إلى تعطل الخادم.
- خداع بعض المســتخدمين في المنظمة عن طريق إرســال «تقرير فصلي» مزيف عبر البريد الإلكتروني وهو في الواقع برنامج ضار يقوم بتشغيل أداة تضر بأجهزة الحاسب الآلي وتؤسس اتصالات بمضيف خارجي.
- مهاجــم يحصل على بيانات حساســة ويقوم بتهديد الرئيــس التنفيذي للشركة بأنه سيجعل البيانات متاحة للعامة إذا لم تقم المنظمة بدفع مبلغ معين من المال.
- مســتخدم يقوم بعرض بيانات حساسة للآخرين من خلال خدمات النظراء لمشاركة الملفات (peer-to-peer).

في الفصول السابقة قمنا بتعريف المكونات الهامة لأمن المعلومات بما في ذلك التهديدات والأصول وخصائصها وبعض التدابير المشــتركة للحد من مشــكلات أمن المعلومات. ولسوء الحــظ فإنه، وعلى الرغم من كل هذه المحاولات، مــن المرجح أن يجد المتطفل طُرقاً لخلق المشكلات. ونُطلق على تلك المشكلات (الحوادث الأمنية). وللاستجابة للحوادث الأمنية، من المفيد تطوير بعض الإجراءات الموحدة وصقل تلك الإجراءات بناء على الخبرات. وســُنقدم في هذا الفصل العناصر الأساسية لإجراءات التعامل مع الحوادث الأمنية.

التعامل مع الحوادث الأمنية:

كيــف يتم التعامل مــع الحوادث الأمنية؟ في الجزء الأول من هذا الكتاب، ألقينا نظرة عامة على المشــكلات التي يتم التعامل معها عند الاستجابة للحوادث، وذلك عندما ناقشنا مشكلة خادم البريد الإلكتروني للطلاب. وبالنظر إلى تلك المشكلة، ما الخطوات التي قمت بها للاستجابة إلى تلك الحادثة؟ ماذا عن الإصابة بالفيروسات، أو تشويه صفحات الشبكة؟ هل هناك إجراءات مشتركة للاستجابة المناسبة لجميع هذه الحوادث؟

في حين أن إجراءات التعامل مع كل حادثة قد تختلف، إلا أن العملية بشــكل عام تبقى كما هي. وهذه الإجراءات موضحة في إدارة مخاطر تقنية المعلومات (rev2 61-NIST 800) وتتضمن ٤ خطوات أساسية:

١. الإعداد.

٢. الاكتشاف والتحليل.

٣. الاحتواء والاستئصال والاسترداد.

٤. تحليل ما بعد الحادث الأمني.



وفي المنظمات الأكثر فاعلية فإن هذه الخطوات لا تستقل بذاتها بل تُعد جزءاً من دورة تُكرر نفسها في كل مرة تواجه المنظمة حدثاً ضاراً. وفي بقية هذا الفصل سنناقش عناصر التعامل مع الحوادث الأمنية التقليدية وذلك باتباع إجراءات إدارة مخاطر تقنية المعلومات (NIST).

مثال مرجعي: التعامل السيء مع الحوادث الأمنية

هذه الأيام، ومع وجود درجة عالية من الاحتراف في عالم تقنية المعلومات، من الصعب الحصول على مثال سيئ للتعامل مع الحوادث الأمنية. ولحسن حظنا فقد قام المفتش العام لوزارة التجارة الأمريكية في السادس والعشرين من يونيو من عام ٢٠١٣ بإصدار تقرير مراجعة للحوادث الأمنية الاستثنائية التي كان التعامل معها تعاملاً سيئاً في إدارة التنمية الاقتصادية (Economic Development Administration) وهي وحدة صغيرة نسبياً في وزارة التجارة الأمريكية حيث بلغت ميزانيتها السنوية ٤٦٠ مليون دولار في عام ٢٠١٢.

وخلاصة القول أن وزارة الأمن الداخلي نبهت إدارة التنمية الاقتصادية (EDA)، وإدارة المحيطات والغلاف الجوي الوطنية (National Oceanic and Atmospheric Administration) في السادس من ديسمبر من عام ٢٠١١ بوجود برامج ضارة محتملة في أنظمتها المعلوماتية. وبحلول الثاني عشر من يناير من عام ٢٠١٢ تمكنت إدارة المحيطات والغلاف الجوي الوطنية من إصلاح مشكلاتها وإعادة أنظمتها المتأثرة إلى الخدمة، أي تقريباً بعد ٣٥ يوماً من التحذير الأولي.

وعلى النقيض من ذلك فإن إدارة التنمية الاقتصادية أصرت على التعهد بإزالة البرمجيات الضارة من جميع أنظمتها الإلكترونية وذلك خوفاً من انتشــار الإصابة بالبرمجيات الضارة وتدخل أحد أطراف الحكومة. ولتحقيق ذلك أنفقت إدارة التنمية الاقتصادية لعلاج المشــكلة أكثر من ٢,٧ مليــون دولار بما في ذلك ١,٥ مليون دولار تكلفة خدمــات من أحد متعهدي تقنية المعلومات. وتُمثل هذه التكلفة أكثر من نصف مجموع الميزانية السنوية لتقنية المعلومات في إدارة التنمية الاقتصادية.

ومــا يثير الاهتمام أكثر أن إدارة التنميــة الاقتصادية دفعت ٤,٣٠٠ دولار للمتعهد ليقوم بتدمير ما كُلفته ١٧٠,٥٠٠ دولار من أجهزة تقنية المعلومات والتي اشتملت على الطابعات وأجهزة التلفزيون، والكاميرات، وأجهزة الحاسب المكتبية، وفارات الحاسب الآلي، وحتى لوحات المفاتيح.

وقد توقف هذا التدمير الوحشي في الأول من أغســطس من عام ٢٠١٢ بســبب اســتنفاد إدارة التنميــة الاقتصادية لمواردها المالية بســبب هــذه الجهود الهدامة. ولهذا فقــد أوقفت إدارة التنميــة الاقتصادية تدمير ما تبقى من مكونات تقنية المعلومات والذي تبلغ قيمتها أكثر من ٣ مليون دولار. وكانت إدارة التنمية الاقتصادية تنوي اســتئناف أنشــطتها التدميرية بمجرد توفر الموارد المالية اللازمة لذلك.

وكل ذلك فقط لإزالة برامج ضارة نمطية أثرت في اثنين مما يقارب من ٢٥٠ عنصراً من عناصر تقنية المعلومات (كأجهزة الحاسب الآلي المكتبية، وأجهزة الحاسب الآلي المحمولة، والخوادم).

وهــذه الحادثة أحد أمثلة ما يمكن أن تتعرض لــه كل مرحلة من مراحل التعامل مع الحوادث الأمنيــة. وسنســتخدم هذا المثال خلال هــذا الفصل من الكتاب لتوضيح الأمور الســلبية التي قــد تحدث. وقد يكون هذا الحادث ظريفاً إن لم تكن تكاليف تلك النتيجة غير الســعيدة من الضرائب التي يدفعها المواطنون.

المراجع:

US Department of Commerce, OIG Final Report, «Economic Development Administration Malware Infections on EDA's Systems Were Overstated and the Disruption of IT Operations
Was Unwarranted,» OIG-13-027-A, June 26, 2013, http://www.oig.doc.gov/OIGPublications/OIG-13-027-A.pdf (accessed 07/14/2013)

الإعداد:

الإعداد هو الخطوة الأولى في وضع خطة الاستجابة للحوادث الأمنية. وينطوي الإعداد على أكثر من محاولة التفكير في جميع سيناريوهات التهديد المحتملة والتي يمكن أن تؤثر في مواصفات أصل معين، والرد المناسب على كل من هذه السيناريوهات. وبدلاً من محاولة أن نكون على استعداد تام للتعامل مع جميع أنواع أنشطة التهديد المختلفة ضد جميع الأصول المختلفة، فإنه من المفيد أكثر أن نقوم بتحديد الخطوات الأساسية المشتركة بين جميع تلك الأحداث والتخطيط لتنفيذ تلك الخطوات.

وضع سياسية للاستجابة للحوادث الأمنية:

تتمثل الخطوة الأولى للتحضير للتعامل مع الحوادث الأمنية في وضع سياسة للاستجابة للحوادث الأمنية والحصول على موافقة الإدارة العليا على تلك السياسة. وتصف سياسة الاستجابة للحوادث الأمنية الطرق الموحدة المستخدمة من قبل المنظمة في التعامل مع حوادث أمن المعلومات. وقد ينظر العديد من الأشخاص إلى هذه الخطوة بأنها عمل غير ضروري إلا أن هذه الخطوة مهمة جداً لمرحلة التنفيذ فيما بعد. وذلك لأن هذه السياسة تساعد على التركيز على الحادثة بأكملها من البداية إلى النهاية دون تشتيت من وسائل الإعلام والضغوط التنظيمية، متضمناً ذلك النتائج المحتملة للضوابط المؤقتة التي قد تضطر إلى وضعها لاحتواء أو استئصال التهديد. على سبيل المثال، إذا تعرض خادم الشبكة الخاص بالجامعة إلى هجوم ما، فإنه من الأفضل أن يكون هناك سياسة تسمح لتقنية المعلومات بتعطيل الموقع الإلكتروني ما دام ذلك ضرورياً للتعامل مع هذه القضية، بدلاً من الاضطرار للحصول على أذونات من أصحاب المصلحة في الوقت الفعلي للقيام بذلك. وفي الواقع فإن معرفة أن الجامعة تتبع إجراءات موحدة سيكون مطمئناً لأصحاب المصلحة بما في ذلك مستخدمي الموقع الإلكتروني مقارنة بمعرفة أن الجامعة تحاول اكتشاف ما يجب عليها القيام به في الوقت الفعلي. كما أن النقاشات المشتركة في تطوير سياسة الاستجابة للحوادث الأمنية تساعد الإدارة على فهم القضايا التي قد تضطر للتعامل معها خلال الحوادث الأمنية الفعلية.

ويجــب أن تكون السياســة في صيغــة مكتوبة لأنها مفهوم مهــم في الأمن وعلى جميع المديرين أن يدركوا أهمية هذا المفهوم. كما أن صعوبات تطبيق السياســة تختلف اختلافاً كبيراً من منظمة إلى منظمة أخرى.

في جامعة جنوب فلوريدا، السياســات تُكتب أولاً، ثم يتم فحصها من قبل وحدة تقنية المعلومات واللجان التوجيهية الداخلية، ثم تنتقل إلى المستشــار العام لفحصها مع الجهات المختلفــة في الجامعة بدءاً من اتحاد أعضاء هيئة التدريس ووصولاً بالموارد البشرية، وذلك لمدة ٨ أســابيع. وميزة هذه العملية المطولة أنها تســاعد على التعريف بالسياســات كما تســاعد على زيادة الوعي الأمني. لكن في المنظمات الأخرى قد تكون رسالة بريد إلكتروني مبســطة إلى المســؤول التنفيذي كافية لتطبيق السياسة. وتجدر الإشارة إلى أن دعم الإدارة العليا نقطة مشتركة في كلا المنهجين ويتوجب أن يكون في أي سياسة.

وهذا هو الســبب وراء الحاجة إلى السياســة في صيغة مكتوبــة: إذا كان من الضروري ســحب القابس من الخادم لأن معلومات حساسة قد تتسرب بسبب أحد المهاجمين، فإنك تريد الاطمئنان التام إلى أن شخصاً ما يدعمك.

والنطاق هو جزء من سياســة الاســتجابة للحوادث الأمنية ويقوم بتحديد أهداف هذه السياســة. ومن المستحســن أن يكــون النطاق ضيقــاً ومحدداً قدر الإمــكان بما هو قابل للتحقيق. وتشــمل عناصر النطاق ما يلي (أ) ما الأصول التي يتم تغطيتها بالسياسة؟ (ب) هل هناك أي استثناءات لهذه السياسة؟ (ج) هل هناك دوائر داخل المنظمة لديها القدرة لرفض الالتزام بالسياسة؟ (د) هل بإمكان الدوائر الفردية أن تكون أكثر خصوصية وصرامة في سياســاتها؟ الجامعات على ســبيل المثال معروفــة باللامركزية من حيــث موارد تقنية المعلومــات. وفي هــذه المنظمات قد يكون من الضروري محاولة التوصل إلى اتفاق بشــأن متى يُصبح الحادث الأمني مصدر قلق على مستوى المنظمة.

ووجود السياســة ليس كافيــاً في حد ذاته بل إن على جميع المعنيــين أن يعرفوا ما هو موجود في تلك السياسة.

وفي حالــة إدارة التنمية الاقتصادية (EDA)، جاء في تقرير مكتب المفتش العام (OIG) النص التالي:

«لم يتفهــم موظفــو وزارة التجــارة التوقعات الســابقة لخدمات الاســتجابة للحوادث المحددة كما هو موضح في اتفاقية مستوى الخدمة (SLA) بين وزارة التجارة وإدارة التنمية الاقتصادية. وهذه الاتفاقية تنص بوضوح على الالتزام بخدمات الاستجابة للحوادث التابعة لوزارة التجارة (مثل التحقيق، والأدلة الجنائية، والهندسة العكسية)، كما تحدد مسؤوليات إدارة التنمية الاقتصادية في الاســتجابة للحوادث (مثل الإبــلاغ عن الحوادث والتعامل مع البرمجيــات الخبيثة المحذوفة والمحجور عليها). ولأن موظفي وزارة التجارة لم يفهموا هذه الاتفاقية، فقد افترضوا بشكل غير دقيق أن إدارة التنمية الاقتصادية قادرة على أداء أنشطة تحليل الحوادث الأمنية (مثل تحديد مدى انتشار البرمجيات الضارة)».

فريق الاستجابة للحوادث الأمنية:

تعمــل المنظــمات على تحيدد موظفــين لوظائف معينــة. ومن المهم أيضــاً أن يكون هناك موظفون محددون للاســتجابة للحوادث الأمنية. ويطلق على هؤلاء الموظفين فريق الاســتجابة للحوادث الأمنية. ومن المعــروف أن الحوادث الأمنية لا تحدث كل يوم، إلا أن موظفي الاســتجابة للحــوادث الأمنية يعملون على تطوير خبراتهم لتتســق مع ما تتوقعه المنظمة خلال الحوادث الأمنية.

إن الهدف الرئيسي لفريق الاستجابة للحوادث الأمنية هو الحماية العامة للبنية التحتية الحاســوبية للمنظمة، ومن ثم فإن على أعضاء الفريق أن يكونوا على معرفة شاملة بهيكلة تقنيــة المعلومات في المنظمة. وبشــكل عام فإن الفريق مســؤول عــن دورة التعامل مع الحوادث الأمنية متضمناً ذلك:

- التحديد السريع لتهديدات البنية التحتية لبيانات الجامعة.
- تقييم مستوى المخاطر.
- اتخاذ خطوات فورية للتقليل من المخاطر التي تُعد حرجة وضارة على تكامل موارد الأنظمة المعلوماتية للجامعة.
- أن يتم إبلاغ الإدارة بالحادثة ومخاطرها.

- أن يتم إبلاغ الموظفين المحليين بأي مخاطر ذات علاقة بالموارد التي يعملون عليها.
- إصدار تقرير نهائي حسب الحاجة، متضمناً ذلك الدروس المستفادة.

ولفريق الاستجابة للحوادث الأمنية أدوار متعددة قبل وأثناء وبعد وقوع الحوادث. ويجب أن يكون دور كل عضو من أعضاء الفريق جزءاً من سياسة الاستجابة للحوادث.

وفي كثير من الأحيان تمر عضوية فريق الاستجابة للحوادث الأمنية من خلال أكثر من إدارة، وعلى المُديرين أن يتفهموا ذلك وأن يوافقوا على سحب أعضاء فريق الاستجابة للحوادث الأمنية من مشاريعهم الحالية وتخصيصهم للفريق الأمني، خصوصاً عندما يتعلق الأمر بمرحلة احتواء الحادث الأمني.

وفي المنظمات الكبيرة قد تكون هناك حاجة لأكثر من فريق للاستجابة للحوادث الأمنية حيث يكون كل فريق في قسم من أقسام المنظمة. وإذا كان من الضروري استخدام فِرَق متعددة، فمن المهم أن تكون هناك مجموعة مركزية مسؤولة عن اتخاذ القرارات الأمنية عندما تبدأ الأحداث بتجاوز حدود القسم المتضرر. على سبيل المثال، الإصابة ببرنامج ضار في أجهزة الحاسب الآلي في كلية الآداب قد تهدد تكامل الشبكة العامة إذا تمت إصابة مناطق أخرى من الحرم الجامعي. إن احتواء انتشار الإصابة في الكلية عن طريق قطع وصول الكلية إلى الشبكة الجامعية أمر يقع ضمن اختصاص المجموعة المركزية لفريق الاستجابة للحوادث الأمنية.

> في جامعة جنوب فلوريدا، تتطلب السياسة وجود إدارات ووحدات منفردة لتنبيه فريق الاستجابة للحوادث الأمنية وذلك عند مشاركة أصل مُصنف بأنه «أصل مقيد» في حدث سلبي. ويجب أن يعمل أعضاء فريق الاستجابة للحوادث الأمنية مع بعضهم البعض في أقرب وقت يتم فيه الكشف عن الحادث داخل الجامعة. وبعد استعادة العمليات العادية، يجب تقديم تقرير لجميع أعضاء فريق الاستجابة للحوادث الأمنية ومسؤولي النظم الداخلية يحدد بوضوح مدى الاختراق والخطوات التي اتخذت لتجنب الحوادث في المستقبل. ويتم مراجعة هذه الحوادث من قبل مدير إدارة أمن تقنية المعلومات كجزء من برنامج تقييم المخاطر المستمر (سيتم مناقشة تقييم المخاطر في الفصل ١٤).

ويكون لفريق الاستجابة للحوادث الأمنية رئيساً واحداً وعادة ما يكون محلل أمني رفيع. وهذا المحلل يقوم بالتنسيق مع أعضاء فريق الاستجابة للحوادث الأمنية ومساعدتهم في أداء وظائفهم عند التعامل مع الحادث الأمني كالتواصل مع الإدارة والمستخدمين وموظفي تقنية المعلومات والموردين ومزودي خدمات الإنترنت وغيرهم. ويتحكم رئيس فريق الاستجابة للحوادث الأمنية بالقضية أثناء تطورها خصوصاً من الناحية التقنية. ولذلك فإنه من الأهمية بمكان أن يكون لهذا الشخص مصداقية عالية داخل المنظمة بسبب كفاءته، ومهاراته الممتازة في التواصل الكتابي والشفهي، وخلفيته التقنية الكافية لفهم القضية، ولقدرته على صنع قرارات لحظية مدروسة ومستندة إلى تحديثات الحالة المعطاة من قبل أعضاء الفريق الآخرين.

ويتم اختيار الأعضاء الفنيين في فريق الاستجابة للحوادث الأمنية بناءً على نشاط التهديد. على سبيل المثال، إذا تم اختراق قاعدة بيانات أوراكل (Oracle) بسبب استغلال حساب أحد مسؤولي النظام على نظام التشغيل، فإن أعضاء فريق الاستجابة للحوادث الأمنية قد يشمل:

- شخصاً مطلعاً على نظام التشغيل وذلك لإلقاء نظرة على نظام التشغيل والسجلات، أو على الأقل استخراج السجلات للتحليل بواسطة شخص على دراية بأدلة البيانات الجنائية.
- مسؤول قاعدة بيانات، وذلك لفحص قاعدة بيانات أوراكل، ومحتوياتها، وسجلاتها في محاولة لتحديد ما إذا تم تغيير شيء ما في قاعدة البيانات.
- مهندس شبكات لمراجعة سجلات الجدار الناري في محاولة لرصد حركة المرور الخارجة عن المألوف.
- يمكن استدعاء موظف خدمات دعم فني إذا كانت الأجهزة المكتبية ستؤدي إلى اختراق حساب مسؤول النظام.

ويجب أن يكون فريق الاستجابة للحوادث الأمنية مؤهلاً، كما يجب على المنظمة أن تستثمر بعض الأموال لمساعدة فريق الاستجابة للحوادث الأمنية في المحافظة على كفاءته.

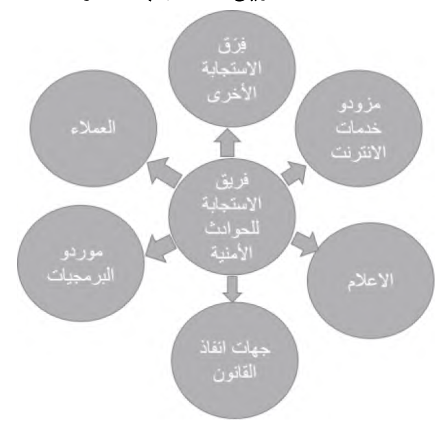
فعندما تسوء الظروف الأمنية فإن فريق الاستجابة للحوادث هو خط الدفاع الأساسي. وفي مثال إدارة التنمية الاقتصادية (EDA)، فقد جاء النص التالي في تقرير مكتب المفتش العام عن فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة:

«إن عدم كفاية خبرة موظفي فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة وعدم معرفتهم بقدرات الاستجابة لحوادث إدارة التنمية الاقتصادية قد أعاق تقديم الإدارة لخدمات الاستجابة الكافية للحوادث. وكان معالج الحادث في فريق الاستجابة للحوادث الأمنية، والذي يدير أنشطة الاستجابة الأولية للحادث، يتصف بالحد الأدنى من خبرات الاستجابة للحوادث، وليس لديه أي تدريب على الاستجابة للحوادث، ولم يكن لديه المهارات الكافية لتقديم خدمات الاستجابة للحوادث. إن قلة الخبرة والتدريب والمهارات أدت بمعالج الحادث لطلب معلومات تسجيل الشبكة الخاطئة (أي القيام بالتحليل الخاطئ للحادث) مما أدى بإدارة التنمية الاقتصادية للاعتقاد أن لديها انتشاراً في البرمجيات الضارة على نطاق واسع ومن ثم الانحراف عن الإجراءات الإلزامية للاستجابة للحوادث. وعلى مكتب المدير التنفيذي للمعلومات التأكد من استيفاء جميع موظفي فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة للحد الأدنى من مؤهلات الاستجابة للحوادث الأمنية».

فريق الدعم:

ما يحدث أثناء الحادث الأمني أكثر من التجسس التقني. فالتواصل جانب مهم من واجبات فريق الاستجابة للحوادث الأمنية. وأحد السمات الخاصة بالحوادث مقارنة بعمليات تقنية المعلومات الروتينية هي الرغبة الجامحة لمختلف الدوائر في الحصول على المعلومات. وغالباً ما تكون هذه الاحتياجات المعلوماتية غير منسجمة معاً. فالمستخدم النهائي مهتم كثيراً بمعرفة موعد استعادة الخدمة، وضابط الامتثال مهتم بمعرفة ما إذا تم اختراق أي من المعلومات. وإذا كان هناك احتمال لاهتمام عام أوسع بالحادثة، فإن وسائل الإعلام تكون مهتمة مباشرة بتعليقات أكبر المديرين التنفيذين في المنظمة وذلك قبل موعد الموجز الاخباري القادم. وعندما تتلقى هذه الاستفسارات فإنه لا يكون لديك غالباً معلومات كافية لتقديم رد على نحو مرضي (الشكل ١١-١).

الشكل (١١-١): تفاعلات فريق الاستجابة للحوادث الأمنية



إن إدارة تدفــق المعلومــات أمــر مهم في مثل هذه الحالات. ومن المهم بشــكل خاص مقاومــة الرغبة بنقل التكهنات على أنهــا رأي الخبير المعني بالأمر. وفي حين أنه من المفيد الاعــتراف بالحوادث خصوصاً تلك الحوادث التي تؤثر في المســتخدم النهائي، فإنه أيضاً من المستحسن اتباع مفهوم «معرفة ما نحتاجه». ومعرفة ما نحتاجه هو مبدأ لإدارة المعلومات يتم بناء عليه توفير المعلومات الضرورية فقط لأداء العمل.

ومبدأ (معرفة ما نحتاجه) لا يعني أن تكون الأحداث سرية، بل إن الاعتماد المتسق على هــذا المبدأ يُقلل من المكالمات غير الضرورية من المديرين لموظفي تقنية المعلومات، وذلك للحصول على معلومات «متميزة». أما بالنســبة للباحثين عن المعلومات فيمكن توجيههم إلى المواقع الإلكترونية أو إلى القنوات الأخرى المحددة في سياسة الاستجابة للحوادث الأمنية.

وقبــل تحديث هذه المعلومات ينبغي على فريق الاســتجابة للحوادث الأمنية النظر في تدخل الإدارة القانونية لاتخاذ قرار بشأن ما يتم الكشف عنه وكيف يتم الكشف عنه. أما من جهة التواصل مع الجمهور، ينبغي النظر في الوحدات التالية:

العلاقــات الإعلاميــة: إذا كان لدى المنظمــة مثل هذه الإدارة فــإن جميع المعلومات التــي يتم تبادلها مع المجتمع خارج المنظمة يجب أن تمر عبر هذه الإدارة لأن لديها الخبرة والدراية في كيفية التعامل مع مثل هذه الحوادث.

المستشـــار القانوني: الإدارة القانونية تتحقق من تطبيق قوانين الإفصاح التابعة للولاية أو للدولة على حدث معين خصوصاً عندما تكون المشكلة ذات علاقة بسرية البيانات. وقد يؤدي الإفصاح غير المقصود إلى عواقب مالية وعواقب عامة قاسية على المنظمة.

إنفــاذ القانــون: في كل جامعة يوجد شرطــة داخلية تابعة للجامعة. ولا يســمح لأي جهة إنفاذ قانون خارجية بالدخول إلى الحرم الجامعي، حتى وكالة الاســتخبارات الأمريكية ومكتب التحقيق الفيدرالي، دون معرفة الشرطة الجامعية والمستشار العام.

وهذه الخطوات تقلل من إمكانية ترويج الشائعات، وترويج الشائعات المجهولة المصدر، والاضطراب العام خلال الاستجابة للحوادث.

مبدأ «معرفة ما نحتاجه» شائع في الإعدادات العسكرية والإعدادات الجاسوسية كوسيلة للحفاظ على أمن الأفراد. وإذا كان العدو يعلم بأن الجندي أو الجاســوس لا يملك معلومات سرية، فإن هناك احتمالاً بسيطاً جداً في أن يقوم العدو في الاستثمار في الجهد المطلوب للقبض على الجندي أو الجاسوس.

التواصل:

سنلقي نظرة على التواصل لأنه يمثل جزءاً أساسياً من الاستجابة للحوادث (شكل ١١-٢).

الإبلاغ عن حادث للمتابعة هناك عدة طرق مختلفة قد تلفت انتباه فريق الاســتجابة للحوادث الأمنية.

في الإبلاغ المباشر، يقوم صاحب الأصول أو القائم عليها بالإبلاغ عن الحادث بنفسه. على سبيل المثال، لنفرض أن لديك عادة حسنة تتمثل في البحث من وقت لآخر عن رقم الضمان الاجتماعــي الخــاص بك في جوجل. وفي أحــد الأيام حصلت على رقــم الضمان الاجتماعي الخــاص بك في ملف وورد يتبع لمقرر دراسي أخذته منذ زمن طويل في جامعتك الســابقة. وكمســتخدم ذكي، ســتقوم مباشرة بالبحث عن الشخص المسؤول عن أمن تقنية المعلومات وتُبلغه بأن رقم الضمان الاجتماعي الخاص بك عرضة للخطر.

والوســيلة الأخرى هي **الإبلاغ المجهول** حيث تُتيح المنظمات إمكانية شــخص ما الإبلاغ عن مشــكلة ما دون الكشــف عن هويته حتى لا يكون خائفاً مــن الانتقام. وأحد الأمثلة على ذلك هي المزاعم بأن مســؤولاً رفيع المســتوى يقوم بطباعة مواد إباحية على طابعات الجامعــة. وهذا الادعاء ســيدق كل أنواع الأجراس في الجامعة بــدءاً من مخاطر العلاقات العامة ووصولاً إلى التحرش الجنسي وانتهاءً بالاســتخدام غير الملائم لأموال الضرائب. وعلى افتراض أن هذا الادعاء صحيح، فمن الواضح أن الموظف لا يرغب في أن يُرى اســمه مرتبطاً بهذا الادعاء خوفاً من فقدان وظيفته.

الشكل (١١-٢): تواصل فريق الاستجابة للحوادث الأمنية

كلية الآداب
- مباشر
- مجهول
- الدعم الفني
- الرقابة الذاتية

فريق الاستجابة للحوادث الأمنية

موجهة لـ
- موظفي تقنية المعلومات
- الإدارة
- المستخدم النهائي
- الامتثال
- الاعلام

مكتــب **الدعم الفني** قد تكون له علاقة بعملية الإبلاغ لأن موظف مكتب الدعم الفني قــد يتعثر بشيء ما أثناء عملية حل المشــكلات الفنية. على ســبيل المثال، تســمح التهيئة الخاطئة لمحرك أقراص الشــبكة المشتركة بمدى كبير من الوصول للمستخدمين دون تطبيق مبدأ «معرفة ما نحتاج إليه». وربما يتلقى مكتب الدعم الفني تقريراً من أحد المستخدمين الــذي عثر على شيء مــا. ويُعد مكتب الدعم الفني جهة إبــلاغ منفصلة وذلك لأن مكتب الدعم الفني يســتلم تذاكر المشــكلات الفنية بحيث يمكن لمجموعة كبيرة من الأشــخاص الاطلاع على محتوى تلك التذاكر. تأمل في كمية التفاصيل التي تراها في تذكرة الدعم الفني الواردة لمكاتب الدعم الفني. وهذا يعود للتحكم في الرسالة ومبدأ «معرفة ما نحتاج إليه».

وأخيراً فإن أساليب **الرقابة الذاتية** مثل تقييم الثغرات الدوري وتحليل السجل قد يؤدي إلى إبــراز بعض الاختراقات التي يجب التعامل معها. وأحد الأمثلة الشــائعة على ذلك هو المســؤول الذي اكتشــف اختراقاً بســبب أن حِمل وحدة المعالجة المركزية لجهاز الحاسب الآلي كان عالياً جداً مما أدى إلى مشــكلات في الجاهزية. وبمجرد استدعاء المسؤول لتحليل المشــكلة اســتنتج بسرعة أن عمليات بروتوكول نقل الملفات (FTP) هي ســبب المشكلة. ويحفظ موقــع بروتوكول نقل الملفات (FTP) ملفات صوتيــة بصيغة (mp3) للمهاجمين

وذلك لمشاركتها مع بعضهم، وهذا الموقع يُستخدم بشكل كبير مما أدى إلى الحِمل العالي في وحدة المعالجة المركزية. وللأسف فإن هذا السيناريو شائع جداً.

الإشـعارات في أكـثر الأحيان يبدأ الأشـخاص في المنظمـة بطرح الأسـئلة عندما تصبح الحوادث الأمنية صعبة الحل. وهذا ينطبق بشـكل خاص على الأشـخاص الأكثر تضرراً من الحادث الأمني. وإذا كان الحادث يؤثر في المديرين والقادة التنفيذين الآخرين فإن الضغط من أجل التواصل السريع واتخاذ قرار يكون أكبر.

ويجب إشـعار **موظفي تقنية المعلومـات وموظفي الدعم الفنـي**، وخصوصاً إذا كان الحادث يؤثر في جاهزيـة الأصول. ويتلقى مكتب الدعم الفني مكالمات هاتفية كثيرة من المسـتخدمين إذا كانت الحادثة تنطوي على أصل من الأصول المهمة و«الضرورية» بالنسبة للمنظمـة. وفي بيئـة تقنيات المعلومـات اللامركزية، مثل العديد مـن الجامعات البحثية في مختلـف أنحاء الولايـات المتحدة، ينبغي أيضاً إبلاغ منظـمات تقنية المعلومات الأخرى ليكونوا على حذر. على سـبيل المثال، إذا كان الحادث يتعلق بهجمات رفض الخدمة التي أصبحت ممكنة بسـبب الثغرات غير المصححة، فـإن الوحدات الأخرى قد ترغب في إجراء تصحيحات طارئة قبل أن تعاني أيضاً من هجمات رفض الخدمة.

كـما يجب أيضـاً إبـلاغ الإدارة أولاً بأول. ومن الجيد إشـعار المديريـن وبقية القادة التنفيذيين بشـكل دوري ولو لم يحدث أي تغيير. وهذا سوف يُقلل من الاتصالات الهاتفية بما فيها تلك المكالمات المباشرة للمهندسـين المفترض تخصيص نسـبة (١٠٠٪) من جهودهم لاحتواء واستئصال المشكلة. ومن المفيد في هذه المرحلة الاستعانة بالرسائل النصية السريعة ورسائل البريد الإلكتروني المختصرة التي توضح تحديثات الحالة.

كما يُصاب المسـتخدم النهائي والعميل بالتوتر عند عـدم معرفتهم بما يجري. ويُطرح في العادة سؤالان أثناء انقطاع الخدمة: متى يعود النظام إلى الخدمة؟ وما الذي حدث بالضبط؟ وفي بعض الأحيان، تكون الإجابة صعبة عن هذين السؤالين. ففي شهر ديسمبر من عام ٢٠١٢ عانت شركة فيسـبوك (Facebook) من انقطاع كبير في الإنترنت بسبب مشكلات في خدمات اسم المجال (DNS). وعلى الرغم من أن انقطاع الخدمة استمر فقط ١٥ إلى ٢٥ دقيقة، فإن المسـتخدمين من جميع أنحاء العالم كانوا مُحبطين ومرتبكين. ويشهد بذلك التغريدة التالية وهي تغريدة من آلاف التغريدات التي أُرسلت خلال انقطاع الخدمة (الشكل ١١-٣).

الشكل (١١-٣): تغريدة لـ (DollSays) أثناء انقطاع خدمة فيسبوك



وللنظر في موضوع سوء التواصل بإمكاننا العودة إلى مثال إدارة التنمية الاقتصادية (EDA) السالف الذكر. وفي الواقع فإن الجزء الأول من التقرير يضع اللوم بشكل كبير على فشل وضعف التواصل بين وزارة التجارة وإدارة التنمية الاقتصادية كما يوضح ذلك النص التالي من التقرير:

أرسل فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة إشعارين إلى إدارة التنمية الاقتصادية بخصوص الحادث الأمني. في الإشعار الأول والذي كان في السابع من ديسمبر من عام ٢٠١١ طلب معالج الحادث في فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة معلومات سجل الشبكة. لكن وبدلاً من تزويد إدارة التنمية الاقتصادية بقائمة الأجهزة التي يُحتمل أن تكون مصابة، قام معالج الحادث وعن طريق الخطأ بتزويد إدارة التنمية الاقتصادية بقائمة تحتوي على ١٤٦ جهازاً داخل حدود شبكتها. وبعد استلام هذا الإشعار اعتقدت إدارة التنمية الاقتصادية أنها تواجه انتشاراً كبيراً للبرامج الخبيثة وأن ذلك أثر في (١٤٦ جهازاً) المدرجة في القائمة.

كما أخطأ فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة في الإشعار الثاني. ففي الثامن من ديسمبر من عام ٢٠١١، قام موظف تابع لشبكة (HCHB) بإبلاغ فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة أن معلومات سجل الشبكة التي طلبها معالج الحادث في فريق الاستجابة لا تحتوي على معلومات عن الأجهزة المصابة. بل إن معلومات سجل الشبكة تحدد فقط أجهزة إدارة التنمية الاقتصادية التي توجد على جزء من شبكة (HCHB). وبعد ذلك قام الموظف التابع لشبكة (HCHB) بالتحليل المناسب حيث توصل إلى أن جهازين فقط يحتويان على سلوك ضار حسب تصنيف مركز استجابة طوارئ الحاسب الآلي الأمريكي (US-CERT). ومع وجود هذه المعلومات الجديدة قام فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة بإرسال إشعار آخر عبر البريد الإلكتروني.

لكن الإشعار الثاني لفريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة كان غامضا، إذ لم يوضح هذا الإشعار أن الإشعار الأول لم يكن دقيقاً. وعلى ذلك استمرت قناعة إدارة التنمية الاقتصادية بوجود انتشار واسع للبرمجيات الخبيثة يؤثر في النظام. وعلى وجه التحديد، فإن بداية الإشعار الثاني كانت تؤكد أن معلومات الإشعار الأول المقدمة عن الحادثة صحيحة.

وعلى ذلك فسرت إدارة التنمية الاقتصادية عبارات الإشعار الثاني بأنها تأكيد للإشعار الأول، في حين قصد معالج الحادث في فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة تأكيد أن إدارة التنمية الاقتصادية هي الإدارة التي تم تحديدها من قبل فريق استجابة طوارئ الحاسب الآلي الأمريكي (US-CERT). وفي الإشعار الثاني لم يقم معالج الحادث في فريق الاستجابة بتحديد أي خطأ أو تغيير في المعلومات المقدمة مسبقاً.

وعلى الرغم من أن مرفقات الإشعار الثاني حَددت بشكل صحيح أن جهازين فقط يحتويان على سلوك مشبوه، وليس ١٤٦ جهازاً كما أفاد سابقاً فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة، إلا أن اسم مرفقات الإشعار الثاني كان يطابق اسم مرفقات الإشعار الأول مما يزيد الوضع غموضاً.

استمر سوء الفهم بين إدارة التنمية الاقتصادية وفريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة لمدة خمسة أسابيع على الرغم من حدوث اتصالات إضافية بين الطرفين، إذ كان لكل منظمة فهم مختلف عن مدى انتشار البرمجيات الضارة. ويعتقد فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة أن هناك جهازين فقط تأثرا بالبرمجيات الضارة، في حين تعتقد إدارة التنمية الاقتصادية بإصابة أكثر من نصف أجهزتها بالبرمجيات الضارة. وقد أسهمت عدة عوامل في حدوث هذه التفسيرات المختلفة:

- افترض فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة أن إدارة التنمية الاقتصادية قد فهمت أن الاشعار الثاني يحل محل الإشعار الأول وأنه لا يوجد سوى جهازين مصابيَن بالبرمجيات الخبيثة. لكن فريق الاستجابة للحوادث الأمنية لم يتابع مع إدارة التنمية الاقتصادية للتأكد من أنها قد فهمت المعلومات الجديدة.

- استجابت إدارة التنمية الاقتصادية للإشعار الثاني بتقديم عينة تتكون من جهازيَن اثنين (من القائمة المرسلة في الإشعار الأول والتي تحتوي على الأجهزة ذات السلوك المشبوه) وذلك لتحليل الأدلة الجنائية. ويعتقد فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة أن هذين الجهازين هما نفس الجهازين المُحددَين في الإشعار الثاني.

- عندما أكد فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة أن عينة الجهازيَن مُصابة بالبرمجيات الضارة، اعتقدت إدارة التنمية الاقتصادية أن فريق الاستجابة للحوادث الأمنية يؤكد إصابة جميع الأجهزة (١٤٦ جهازاً) الموجودة في قائمة الإشعار الأول بالبرمجيات الخبيثة.

- لم يحتفظ فريق الاستجابة للحوادث الأمنية التابع لوزارة التجارة بالإشعار الأول الذي كان يوضح قائمة تحتوي على (١٤٦ جهازاً)، كما أنه لم يوثق الأنشطة الأولية للاستجابة للحادث. وعلى ذلك فإن إدارة فريق الاستجابة للحوادث الأمنية، عندما تَدَخَلت في أنشطة الاستجابة للحادث، لم تر أي سوء فهم قد وقع بين الطرفين.

الامتثال:

الامتثـال هو عملية اتباع القوانين، والأنظمة، والقواعد، والرموز القياسـية، والالتزامات التعاقديـة. ومن الناحيـة المثالية تُعد متطلبـات الامتثال أفضل الممارسـات التي طُورت لتجنـب أخطاء الماضي المعروفـة. لكن من الناحية العملية، الامتثال مهم لأن عدم الامتثال يـؤدي إلى عقوبات يمكن تجنبها. وفي جميع الحالات عليك أن تكون على معرفة بمتطلبات الامتثال المرتبطة بالاستجابة للحوادث الأمنية والتي تنطبق على الوضع الذي أنت فيه، كما عليك التصرف وفقاً لتلك المتطلبات.

وكمثـال على متطلبات الامتثال المرتبطة بالاسـتجابة للحوادث، فـإن قانون إدارة أمن المعلومـات الفيدرالي (Federal Information Security Management Act)[1] يتطلب وكالات اتحادية لتنمية قُدُرات الاستجابة للحوادث الأمنية. ويُطلب من كل وكالة اتحادية مدنيـة أن تعين نقطة تواصل أولية ونقطة تواصل ثانويـة (point of contact) مع فريق استجابة طوارئ الحاسب الآلي الأمريكي (US-CERT)[2]، والإبلاغ عن الحوادث بما يتفق مع سياسة الاستجابة للحوادث التابعة للوكالة.

وكمثال على الامتثال لقانون إدارة أمن المعلومات الفيدرالي (FISMA)، فإنه عند التأكد أو الاشتباه بضياع أو سرقة أو اختراق (معلومات تُحدد الهوية الشخصية) في أنظمة البحرية الأمريكية يُطلب من إدارة البحرية ما يلي:

- استخدام نموذج (13/OPNAV Form 5211) للإبلاغ الأولي ولإنشاء تقارير المتابعة.
- إرسـال النموذج إلى فريق اسـتجابة طوارئ الحاسـب الآلي الأمريكي (US-CERT) خلال ساعة واحدة من حدوث الاختراق.
- إبلاغ مكتب الخصوصية التابع لمدير تقنية المعلومات في البحرية الأمريكية (DON CIO) خلال ساعة واحدة.
- إبلاغ مكتب الدفاع عن الخصوصية (Defense Privacy Office).

---

(1) http://csrc.nist.gov/groups/SMA/fisma/index.html

(2) http://www.us-cert.gov/

- إبــلاغ البحرية الأمريكية (Navy)، أو مشــاة البحرية الأمريكية (USMC)، أو مكتب البحرية للطب والجراحة (BUMED) تبعاً للتسلسل القيادي وحسب مقتضى الحال.

الأجهزة والبرمجيات:

مــن أجل أن يكون فريق الاســتجابة للحــوادث الأمنية فعالاً في عملــه يحتاج للأدوات المناســبة لذلك. وتشــمل عينة الأجهــزة والبرمجيات التي أوصت بهــا إدارة مخاطر تقنية المعلومات (NIST 800-61 rev2) للاستجابة للحوادث ما يلي:

- أجهزة النسخ الاحتياطي وذلك لإنشاء صور للقرص أو للبيانات الأخرى للحادثة.
- أجهزة حاسب آلي محمولة لجمع وتحليل البيانات وكتابة التقارير.
- مكونــات احتياطية لأجهزة الحاســب الآلي لأغراض «التحطــم والإحراق» (crash and burn) مثــل تجربة البرمجيات الضارة وغيرها من الأحمال الحاســوبية «غير المعروفة».
- مُحللات الحزم لالتقاط وتحليل مرور الشبكة.
- برمجيات تحليل الأدلة الجنائية الرقمية لاستعادة البيانات التي تم إزالتها، وتحليل تعديلات الوصول، وإنشاء الجداول الزمنية (MAC)، وتحليل السجل، وغيرها.
- ملحقات جمع الأدلة مثل الكاميرات الرقمية، ومســجلات الصوت، ونماذج تسلسل العهدة، وغيرها.

وأحد أفضل أصدقائك خلال هذه العملية هو محرك البحث. على سبيل المثال، القصاصة البرمجية الخاصة بتســجيل الدخول، وشعار بروتوكول نقل الملفات (FTP) قد تكشف عن معلومات قيمة مثل موقع ملفات السجل، وموقع ملفات التهيئة، وغيرها من الأدلة الهامة التي تساعد الفريق الأمني على بناء جدول زمني متكامل لهذا الحادث.

مــن بين ٨٥٥ حادثاً أمنياً تــم تحليله في تقريــر (Verizon Data Breach Report) لعام ٢٠١٣، اتضــح أن (٨١٪) مــن بين تلك الحــوادث احتوت على اخــتراق، و(٦٩٪) منها تضمنت برمجيــات خبيثة، في حين أن (٦١٪) من تلك الحوادث احتوت على مزيج من الاثنين معاً. ومن ثم فمــن الطبيعي افتراض أن أعضاء فريق الاســتجابة للحوادث الأمنية سيشــاركون في معظم الأوقات في تحليل اختراق أو انتشار لبرمجيات خبيثة مما يستدعي استخدام الأدوات المتخصصة على نطاق واسع. ولهذا خصصنا فصلاً كاملاً لهذا التحليل.

التدريب:

عالم تقنية المعلومات في تغير مستمر. فالتقنيات الجديدة والاختصارات الجديدة تواكب أصــول جديــدة وتهديدات جديدة. وتتمثل وظيفة المحلــل الأمني في الحفاظ على معرفة الأصــول والتهديدات الجديدة خصوصاً تلــك التي تُعرِض المنظمة للمخاطر. وقد يتخصص البعــض في مجال محدد من المجالات الأمنية كتحليــل الأدلة الجنائية، لكن يجب أن يكون لدى الأعضاء الأساســيين في فريق الاستجابة للحوادث الأمنية معرفة عامة بجميع الجوانب الأمنيــة. ويجــب أن يكون الأعضاء قادرين على الابتعاد عــن وظائفهم اليومية والانضمام لوظائف الفريق الأمني، كما يجب أن يكون لديهم نظرة شاملة للمنظمة والأصول والضوابط والتهديدات والنتائج.

وتُعد الشــهادات الأمنية بدايــة جيدة، وذلك ليس لأنها تحتفــظ بمئات الصفحات من المعلومــات التــي تُلقى عليك، مثل الذي يُطلب منه أن يــشرب من خرطوم المياه، بل لأنها توفــر مجموعة من المعلومات الأساســية في جميع جوانب الأمن خصوصاً الأشــياء التي لم تخطر ببالك إلى الآن. وتُبنى الشــهادات الجيدة على المعلومات التمهيدية المُقدمة في هذا الكتاب.

وأحـد الشـهادات المُقدمة مـن منظمة (ISC) هـي شـهادة (Certified Information System Security Professional) أو اختصاراً (CISSP). وهذه الشهادة تعتمد على ما يُعرف بالمعـارف العامـة (Common Body of Knowledge) أو المعلومات الهامة للمتخصصين في أمن المعلومات في جميع أنحاء العالم بما في ذلك:

ضوابط الوصول.

أمن الشبكات والاتصالات.

حوكمة أمن المعلومات وإدارة المخاطر.

تطوير تشفير البرمجيات.

تصميم وهيكلة أمن المعلومات.

العمليات الأمنية.

استمرارية الأعمال والتخطيط للتعافي من الكوارث.

اللوائح والقوانين والتحقيقات والامتثال.

الأمن المادي (البيئي).

الجوانب الأخرى من التدريب تسـتحق الاهتمام أيضاً. فموظفو العلاقات العامة، على سبيل المثال، يجب أن يكون لديهم تعليمات حول كيفية التعامل مع وسائل الإعلام متضمناً ذلك التحكم في الرسـالة وأهمية عدم الكشـف عن المعلومات الحساسة. إن الكشف عن التفاصيل التقنية فيما يتعلق بكيفية اكتشـاف انتشـار البرمجيـات الخبيثة والتحكم فيها، على سـبيل المثال، قد تُنبه قراصنة الحاسـب ومطوري البرمجيات الخبيثة إلى كيفية تجنب نفس الضوابط في الإصدارات المستقبلية للبرمجيات الخبيثة. وفي بعض الحالات يكون ذلك التحكم في الرسـالة معاكسـاً لمبدأ التواصل الفعال والكامل مع الجمهور. وتقوم العلاقات العامـة بعملية الموازنة عندما يتعلق الأمر بالاسـتجابة للحوادث، بشـكل مشـابه لتطبيق الضوابط الأمنية: الكشـف عن الكثير قد يكون مشـكلة، والكشـف عن القليل قد يجعل الأمور تزداد سوءاً.

الاكتشاف والتحليل:

الخطوات في القســم الســابق تضمن أن المنظمة مستعدة للحادث الأمني عند حدوثه. وفي هذا القسم سننظر في العملية العامة لاكتشاف وتحليل الحوادث الأمنية. وسوف نلقي في الأقسام اللاحقة من هذا الكتاب نظرة تفصيلية على بعض تقنيات تحليل الحوادث.

التوثيق الأولي:

وفقــاً لإدارة مخاطر تقنية المعلومــات (NIST 800-61 rev2)، يجب أن يتأكد أعضاء فريق الاستجابة للحوادث الأمنية أن توثيق الحادث يتم بالشكل الصحيح، وأن التوثيق يبدأ عند اكتشــاف الحادث مباشرة. وبينما يتطور التوثيق أثناء عملية الكشف والتحليل، يجب أن يحتوي توثيق الحادث على الأقل على معلومات حول العناصر التالية:

- الوضع الحالي للحادث (جديد، متقدم، تم إرساله للتحقيق، تم حله، وما إلى ذلك).
- ملخص الحادث.
- المؤشرات المتعلقة بالحادث.
- الحوادث الأخرى ذات العلاقة بهذا الحادث.
- الإجراءات التي تم اتخاذها بشأن هذا الحادث من قبل جميع معالجي الحوادث.
- تسلسل العهدة، إذا كان ذلك قابلاً للتطبيق.
- تقييم الأثر المتعلق بالحادث.
- معلومات الاتصال للأطراف المعنية الأخرى (مثلاً مالك النظام، مسؤولي النظام).
- قائمة الأدلة التي جُمعت خلال التحقيق في الحادث.
- ملاحظات معالجي الحادث.
- الخطوات التالية التي يجب اتخاذها (مثلاً إعادة بناء المضيف، ترقية التطبيق).

اكتشاف الحادث:

فيما ســبق مــرّت المنظمة بعملية التحضير للحادث الأمني. وقــد تم القيام بالتخطيط والتدريب وشراء بعض المشتريات. كما تم إعداد التحليل الخاص بالأجهزة، وتهيئة العلاقات العامة. ولسوء الحظ فإن فريق الاستجابة للحوادث الأمنية لن يضطر للانتظار كثيراً لوضعه عــلى المحــك. ولكن كيف ســتدرك المنظمة أن هنــاك أمراً ما ليس طبيعياً؟ وكيف ســيتم الكشف عن الحادث؟

التغييرات المرئية للخدمات:

إن أحد أكثر الطرق شــيوعاً لاكتشــاف الأخطاء في الأنظمة أو البيانات في المنظمات هي اكتشــاف التغييرات المرئية في النظام أو البيانات. ويعد تشــويه مواقع الإنترنت مثال على ذلك. على ســبيل المثال، سوف يلاحظ مستخدم الموقع الإلكتروني بسرعة أن هناك أمراً غير طبيعي عند زيارة موقع إلكتروني ويتم استقباله بالصفحة الموضحة في الشكل (١١-٤).

الشكل (١١-٤): مثال على تشويه موقع إلكتروني



ووفقــاً لتقرير اختراق البيانات (VERIS) لعــام ٢٠١٢، فإنه يتم الإبلاغ عن (٩٢٪) من الاختراقــات بواســطة طرف ثالث. ولأن هذه النســبة المئوية مهمة جــداً، دعنا نضعها في منظور عملي. فبغض النظر عن نوع البرمجيات التي يحاول مورد البرمجيات الأمنية إقناعك بأنها «الحل الســحري» لحماية أصول المنظمة ومراقبتها، هناك نســبة كبيرة أن يتم الإبلاغ بواسطة طرف ثالث عند حدوث اختراق.

مراقبة الأداء:

أما الســيناريو التقليدي الآخر فهو التأثير على الأداء. وفي بعض الأحيان، ونتيجة مباشرة أو غير مباشرة للبرمجيات الخبيثة المثبتة بواسطة قراصنة الحاسب، قد يصبح نظام الحاسب الآلي بطيئاً بحيث يكون ذلك ملحوظاً من قبل المستخدمين أو مسؤولي النظام.

وأحد الاســتخدامات الشائعة لأجهزة الحاسب الآلي المخترقة هو استخدامها في التخزين وجعلها كمستودع بيانات، إما للتبادل غير المشروع لملفات الموسيقا والأفلام، أو لتبادل المواد الإباحية. ويبدو أن تبادل المواد الإباحية قد حصل على الكثير من الاهتمام من قبل قراصنة الحاسب ومن قبل المندسين (lurkers) (وهم الأشخاص الذين يترددون على دوائر القرصنة لكن لا يقومون بمشاركة البيانات).

وبمجرد أن يتعرض جهاز الحاســب الآلي لبرمجيات خبيثة ويتم مشاركة مواد إباحية عن طريق ذلك الجهاز، سيلاحظ المستخدم بسرعة أن أداء الجهاز قد انخفض لأن معظم وحدة المعالجة المركزية وعرض النطاق الترددي لشــبكة الحاســب الآلي تُســتخدم في تحميل تلك المواد. وهذا يتطلب عادة استدعاء مكتب الدعم الفني.

فهم السلوك الطبيعي

من أجل اكتشــاف الأمور غير الطبيعية، على مسؤولي النظام أولاً فهم السلوك الطبيعي للنظام. مثلاً تُســتخدم بعض أجهزة الحاســب الآلي المكتبية في الجامعة من الســاعة الثامنة صباحاً إلى الســاعة الخامســة مســاءً من يوم الإثنين إلى يوم الجمعة فقط. لذلك فإن اكتشــاف محاولة تســجيل دخول لتلك الأجهزة في الســاعة الثانية صباحاً من يوم الســبت يجب أن يُطلق جميع أنواع الإنذارات التحذيرية.

مراقبة المعلومات الشخصية:

ونتيجة مباشرة لجميع الاختراقات الكبيرة في المنظمات الضخمة والتغطية الإعلامية لتلك الهجمات، أصبح الأشــخاص أكثر اهتماماً بمعلوماتهم الشــخصية. وكجزء من هذه العملية، قد يلجأ المســتخدمون إلى استخدام جوجل أو أي محرك بحث آخر للبحث عن معلوماتهم الشخصية مثل رقم الضمان الاجتماعي (الشكل ١١-٥).

الشكل (١١-٥): البحث عن المعلومات الشخصية

وكان من الشــائع قبل عشر ســنوات أن يقــوم أعضاء هيئة التدريــس بتعليق درجات طلابهم على أبواب مكاتبهم. وبدلاً من اســتخدام الأســماء من أجل حماية هوية الطالب، كان أعضاء هيئة التدريس يستخدمون أرقام الضمان الاجتماعي.

الآن وبعــد مرور عشر ســنوات، ما زال لدى أعضاء هيئــة التدريس نفس وثائق الوورد (MS Word) التي كانوا يســتخدمونها ســابقاً لإلصاقها على أبواب مكاتبهم والتي تحتوي على أرقام الضــمان الاجتماعي والدرجات. وفي بعض الأحيان، ينتهي المطاف بهذه الملفات المنسية في أماكن تقوم محركات البحث بالتقاطها وعرضها للعالم.

خدمة تنبيهات جوجل

خدمة تنبيهات جوجل هي أداة تقدمها جوجل لمساعدة المستخدمين على تعقب الموضوعات ذات الاهتمام. ويتمثل الاستخدام الجيد لهذه الأداة من خلال إعدادها لتقدم لك تنبيهاً في كل مرة يتم فيها فهرســة اسمك بواســطة محرك البحث جوجل. مثلاً بإمكانك إدخال الاستعلام (John Doe) ومن ثم توجيه خدمة تنبيهات جوجل لإرسال رسالة بريد إلكتروني في كل مرة يتم فيها العثور على صفحة إلكترونية جديدة تحتوي على هذا الاسم.

مراقبة سلامة الملفات: أدوات سلامة الملفات هي تطبيقات برمجية تراقب سلامة الملفات في نظام أجهزة الحاسـب الآلي. وإذا تم إحداث تغييرات في أحد الملفات، فإنه سـيتم إخطار مسؤول النظام على الفور. وغالباً ما تكون هذه الأدوات جزءاً من الحزمة البرمجية المعروفة بأنظمة اكتشـاف التسـلل المعتمدة على المضيـف (Host-based Intrusion Detection Systems) أو اختصـاراً (HIDS). وهـذه الأنظمة معتمدة عـلى المضيف لأنها تعمل على جهاز الحاسـب الآلي المضيف، وذلك في مقابل أنظمة اكتشاف التسلل المعتمدة على الشبكة (Network-based Intrusion Detection Systems) والتي يشار إليها عادة بـ (IDS).

خذ على سـبيل المثال حالة تشـويه مواقع الإنترنت. فإذا تم مراقبـة صفحة (index.html) (أو الملف الأسـاسي الذي يعادلها) بواسطة أدوات سلامة الملفات، فبمجرد أن تتأثر سـلامة الصفحة (من خلال تغيير المحتوى) سـيتم إشـعار مسـؤول النظام فوراً. وتحتوي العديـد من هذه الأدوات على خيار لاسـتعادة الملف تلقائياً عندما يتم اكتشـاف التغيير. ومن الأمثلة الشـائعة عـلى الأدوات التي تحتوي على تطبيقات لمراقبة سـلامة الصفحات: (OSSEC) (الشكل ١١-٦)، و (Samhain)، و (Tripwire).

الشكل (١١-٦): أداة شائعة الاستخدام في مراقبة الملفات (OSSEC)

وتُلقـي أدوات (مراقبة سـلامة الملفـات) الضوء على مفهوم الإيجـابي الخاطئ (False Positive). والإيجـابي الخاطئ هو الاكتشـاف الذي يبدو أنه مشـكلة (إيجابي) لكن عند

إجراء المزيد من التحقيقات يتبين أنه ليس بمشــكلة (أي يكون خاطئاً). وقد تعلمت أيضاً هذا المفهوم في مجال الإحصاء بوصفه خطأ من النوع الثاني. وهذا المفهوم موجود في العديد من أدوات «الاكتشاف الأمنية» بدءاً من الجُدُر النارية ووصولاً إلى ماسحات الثغرات.

والآن ســنُنُاقش موضوعــاً ذا علاقة بمفهوم الإيجابي الخاطئ في أدوات ســلامة الملفات. فعند تثبيت الأداة يتم سؤال مسؤول النظام عن الملفات التي يجب مراقبتها. وهذا القرار يجب اتخاذه بعناية. على ســبيل المثال، ما الذي ســيحدث إذا قررت مراقبة ســلامة ملف سجل الوصول التابع لخادم الشبكة؟ ملف سجل الوصول التابع لخادم الشبكة يتغير في كل مرة يقوم شــخص ما بزيارة موقعك الإلكتروني. وعلى ذلك فإن أجراس التحذير ســتعمل في كل مرة يكون لديك زائر - وهذه الإنذارات من نوع إيجابي خاطئ.

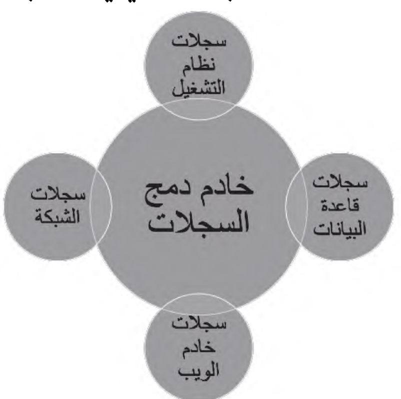
وفي حــين أن ذلك قــد يكون «حســناً» في المواقــع الإلكترونية البطيئة، أمــا في المواقع الإلكترونية الأكثر انشــغالاً فإنك ســتقوم سريعاً بإهمال تلك التحذيرات. إذاً هل يســتحق ذلــك الملــف المراقبة؟ الإجابة كلا. لكن ماذا عن مراقبة ملــف التهيئة؟ أو ملف (index.html) على موقع الإنترنت؟ هذه الملفات قد تستحق المراقبة.

الإبــلاغ من شــخص مجهول: في بعض الأحيان قد يتردد الأفــراد في الإبلاغ عن الأحداث الســلبية خوفاً من الانتقام. ومعظم المنظمات لديها وســائل للإبلاغ عن الأحداث المحتملة أو الأحــداث المُتصــورة دون تحديد هوية المُبلغ. وقد تشــمل هذه الأحداث على ســبيل المثــال، حوادث الاحتيال المحتملة، والاســتخدام غير الملائم للبنية التحتية الحاســوبية من قبل المُديرين وغيرهم من الموظفين الإداريين، وادعاءات التحرش الجنسي على رسائل البريد الإلكتروني، وغيرها.

وفي كثير من الحالات، تتطلب السياســات الداخلية للمنظمة القيام بتحقيق عند استلام أي مــن تلك الادعــاءات عبر آليات الإبــلاغ المجهولة المصدر. وفي حــين أن اتباع مثل تلك السياســة في العالم المثالي أمر جيد، إلا أنه يجب على المنظمات أن تكون ملتفتة إلى حقيقة أن الأفــراد ذوي المناصب غير محبوبين في بعــض الأحيان. إن الاتباع الأعمى والمتكرر لتلك الادعاءات دون التحقق المناســب يمكن في حد ذاته أن يكون تهديداً ضد الأصول الوظيفية (المدير على سبيل المثال) مما يضع المنظمة في خطر.

تحليل الســجل: وهي عبارة عن ســجلات أداء الجهاز. والسجلات هي أفضل أصدقاء المحلل الأمني. وبخصوص اكتشــاف الحادث الأمني، تُســتخدم السجلات من قبل مسؤولي الأمن لتحديد الوقت الذي تعرض فيــه النظام للهجوم، وتحديد الإجراءات التهديدية التي استُخدمت من قبل قراصنة الحاسب (الشكل ١١-٧).

الشكل (١١-٧): السجلات التقليدية المدمجة



وفي نظام لينكس تقع معظم الســجلات في دليــل (/var/log). كما يمكن التحكم في معظم ســجلات نظام التشــغيل من خلال حارس (syslog). والرسائل الموجودة في دليل (/var/log) هي أول ما يقوم المحلل الأمني بتحليله بحثاً عن المخالفات الأمنية مثل رسائل الخطأ الغريبة، وإعادة التشــغيل غير النظامي، وغيرها. وســنتناول تحليل السجلات بمزيد من التفصيل في الفصل اللاحق (الشكل ١١-٨).

وبخصوص عملية الاكتشــاف، قد يكون لدى منظمتك أحد حلول دمج الســجلات (Log Consolidation) أو يكــون لديهــا مديــر متكامــل للحوادث الأمنيــة (Security Incident Event Manager) أو اختصــاراً (SIEM). في حالــة اســتخدام أحد حلول دمج الســجلات، فإنه يتم دمج السجلات من أنظمة وتطبيقات متعددة في خادم منفصل، وذلك للمراقبــة والتحليلات الأمنية وتحليلات الأداء. أما عند اســتخدام أنظمــة المدير المتكامل للحــوادث الأمنية (SIEM) فإنه يتم ضم الدمج مع التحليل حيث تبحث تلك الأنظمة عن الأنماط الشاذة في الأنظمة المتعددة لتحديد التهديدات والاختراقات المحتملة.

وحتى يكون تحليل الســجل فعالاً من المهم تزامن جميع الســاعات في جميع الخوادم التي تُغذي ســجلاتها إلى خادم دمج الســجلات. وهذا التزامن مهم حتى يمكن التأكد من أن تفسير الجداول الزمنية تم بالشكل الصحيح، وذلك عند قيام قراصنة الحاسب باستطلاع ومهاجمة واختراق أنظمة متعددة. نظأنظذأ،ظ

الشكل (١١-٨): تحليل السجلات



ولدمج الســجلات ميزة أخرى. فبالإضافة إلى إمكانية النظر في ســجل الأحداث في مكان واحد مما يجعل من السهل تحليل البيانات للبحث عن حوادث محددة، فإنه يتيح أيضاً نسخ بيانات الســجل إلى خادم آخر مما يحافظ على ســلامة الســجل. وهذا مفيد بشكل خاص عند البحث عن أدلة الاحتيال الذي يرتكبه أشخاص يملكون امتيازات إدارية. وبشكل عام فإن مدير قواعد البيانات يســتطيع تغطية آثاره في خادم قواعد البيانــات، لذا فإن أذونات مدير قواعد البيانات على خادم دمج السجلات أو خادم (SIEM) ينبغي أن تكون أذونات قراءة فقط.

لوحـات إدارة حماية نقطة النهاية: حماية نقطة النهاية (End point protection) أو اختصاراً (EPP) هي صورة متطورة من برمجيات الحماية من الفيروسـات. وحماية نقطة النهايـة تعني أكثر من مجرد رقابة وحماية نظام الحاسـب الآلي من الإصابة بالفيروسـات. وعادة تشمل حلول حماية نقطة النهاية ما يلي:

- الحمايـة من الفيروسـات والبرمجيات الخبيثـة التي «تحاول تثبيت نفسـها» في جهاز الحاسـب الآلي، وتعـرف هذه الحمايـة عادة بحمايـة «الوصول» أو حمايـة «الوقت الحقيقي».
- الحماية من الفيروسـات مع قدرة إزالة و/أو عزل الملفات التي يتم العثور عليها في جهاز الحاسب الآلي، والتي تم تحميلها من الإنترنت، سواء تم تثبيتها أم لم يتم ذلك، من خلال المسح «عند الطلب» أو المسح «المُجدول».
- حماية الجُدُر النارية.
- كشف التسلل المعتمد على المضيف (اختياري).
- سلامة الملفات (اختياري).
- سرقة الهوية (اختياري).
- مراقبة وصول الأطفال (اختياري).

وكما ترى فإن مجموعات حماية نقطة النهاية (EPP) تختلف عن المجموعة المخصصة فقـط للحمايـة من البرمجيات الضـارة. وفي كثير من الأحيان فـإن مجموعة حماية نقطة النهاية (EPP) تحتوي على «روابط» لإدارة تطبيقات الخوادم الأخرى مثل البريد الإلكتروني، وخوادم الشـبكة وغيرها، مما يجعلهـا قريبة من حلول أنظمة المديـر المتكامل للحوادث الأمنية (SIEM). وفي حين أن التكلفة والجهد لتثبيت وتهيئة نظام (SIEM) أو نظام دمج السـجلات تكون مانعاً لكثير من المنظمات، فـإن حماية نقطة النهاية (EPP) تكون متاحة بسـعر تراخيصها. ولأن المنظمات الصغيرة تسـتثمر في حماية نقطة النهاية، فإن لدى تلك المنظـمات الخيار في اسـتخدام مجموعات حماية نقطة النهايـة للقيام ببعض مهام تحليل السجلات (الشكل ١١-٩).

الشكل (١١-٩): مثال على حماية نقطة النهاية



التحقيقات الداخلية: وأخيراً تجدر الإشــارة إلى تلك الأحداث التي يتم العثور عليها من قبــل التحقيقات الداخلية. وجدير بالذكر أننا نتحدث عن التحقيقات التي تنشــأ من قبل قسم التدقيق الداخلي، أو مدققي الولاية (إذا كان العمل في وحدة تابعة للولاية)، أو الموارد البشرية، أو شرطة الجامعة، أو المستشار العام. وفي بعض الأحيان قد تبدأ تلك التحقيقات بشيء بعيد تماماً عن المنطقة التقنية لكن يحتاج إلى مســاعدة إدارة تقنية المعلومات لمزيد من الأدلة. على سبيل المثال، إذا قام موظف مفصول من منظمتك بمقاضاة المنظمة بسبب إنهاء العمل بصورة غير نظامية، فإن المستشار العام قد يطلب منك جمع كل رسائل البريد الإلكتروني التي تمت بين المديرين التنفيذين في المنظمة والتي تم فيها مناقشة هذا الموضوع.

وهنــاك احتــمال آخر بأن يقوم المدقق الداخلي بالتحقيــق في عمليات الإدارة وأن يجد (معلومات تُحدد الهوية الشــخصية) محفوظة في النظــام دون موافقة المكتب الأمني مما يخالف سياسة المنظمة. وفي هذه الحالة، من المهم العثور على جميع المعلومات المحفوظة بشكل غير منظم وتصنيفها وتطبيق الضوابط المناسبة قبل القيام بالتدقيقات الأخرى (مثل تدقيــق البطاقات الائتمانية التابع لصناعة بطاقــات الدفع- Payment Card Industry). كما يتطلب معرفة المشكلات الخطرة الأخرى التي تهدد البيانات.

تحليل الحوادث الأمنية:

بمجرد أن يكون هناك اتفاق على «حدوث مشــكلة أمنية» فإن فريق الاســتجابة الأمنية سيبدأ في عملية تحليل الحادث. والهدف من التحليل هو اكتشاف جميع الأحداث السلبية التي تشــكل منهــا الحادث من أجل الإدارة الفعالة والصحيحــة للمرحلة المقبلة - الاحتواء والاســتئصال. وإذا لم يتم تحليل الحادث بشكل دقيق، فإن المنظمة قد تتعثر في دائرة من الاكتشــاف والاحتــواء في كل دورة مما قد يجلب الضرر عــلى خصوصية وتكامل وجاهزية الأصول المعنية.

ومن الواضح أن التحليل ســيتغير تبعاً لتغير الحالــة، وفي الحياة العملية يجب أن تحاول قياس العائد الذي يمكن أن تحصل عليه من التحليل. على ســبيل المثال، دعنا نفترض وجود انتشــار لبرمجيات خبيثة في أجهزة الحاســب الآلي في قســم الكيمياء. وعلى ما يبدو أنه تمت إصابــة عشرة أجهزة في المختبر مفتوح الاســتخدام بنفس ســلالة البرمجيات الخبيثة. واتضح أن جميع الأجهزة احتوت على الباب الخفي نفســه، والروبوتات نفســها، ورقم المنفذ نفسه. وإذا كان لديك الوقت والموارد المتاحة، فإنه من المناســب أن تُلقي نظرة فاحصة على جميع الأجهزة، وتبحث عن جميع سجلات الأبواب الخفية، وتتأكد مما إذا كان هناك أي آثار لتواصل بــشري حقيقي في اســتخدام النظام. من جهة أخرى، ولأن الأجهــزة كلها في المختبر مفتوحة الاستخدام وليس فيها أي بيانات شخصية، فإنه من الأسهل فحص عينة واحدة من الأجهزة.

وتُعــد محركات البحــث على الإنترنت مصدراً مهم للمعرفة التي يمكن الاســتفادة منها بســهولة من خلال الحصول على معلومات أثناء التحليل. ويمكن البحث عن كل شيء بدءاً من لافتات برتوكول نقل الملفات (FTP) وانتهاءً بالروبوتات، وذلك للحصول على معلومات بخصوص تثبيت البرامج الخبيثة المعينة.

وأخيراً، وكجزء من التحليل، يجب أن تكون قادراً على تحديد المستفيدين، وكذلك تحديد الأصــول المقيدة والأصول الأساســية التي يمكــن أن تتأثر من جراء الحــادث الأمني. هذه الأصول ســتكون أهدافك الرئيسية التي تتطلب حماية واستئصالاً وفقاً للمرحلة التالية من إدارة الحوادث الأمنية.

الاحتواء والاستئصال والاسترداد:

الاحتواء: هو منع انتشــار الضرر، وعادة ينطوي ذلك على فصل أجهزة الحاســب الآلي المصابــة من الشــبكة. وفي العديد من الحوادث الأمنية نصــل إلى نقطة من خلال التحليل يســتحق فيها القيام بالاحتواء قبل أن يتم الانتهاء من كامل التحليل. وهذا يحدث عندما يكون المُحلل واثقاً من أن الأحداث الجارية تســتحق اتخاذ إجراء معين، و/أو عندما يحدد المحلل أن الخطر على الأصول عالٍ جداً في حال استمرار الأحداث كما هي. وبما أن الاحتواء ينطــوي على إغلاق مؤقــت للخدمات، فإن هذا القــرار يحتاج إلى تفكير متــأنٍ في موازنة الخســائر المتوقعة من الخدمات المتعطلة بالخسائر المتوقعة من انتشار الضرر إلى الأجهزة الأخرى. وهذا التفكير نفســه المتأنِ يكون مطلوباً عندما ننظر في عملية الاســتئصال والتي يمكن تعريفها بأنها إزالة الأسباب التي أدت إلى الاحداث السلبية (الشكل ١١-١٠).

الشكل (١١-١٠): الجدول الزمني للاحتواء والاستئصال والاسترداد

الاحتواء
الاستئصال
الجدول الزمني لتحليل الحادث
الاستئصال
الاسترداد

وبالعــودة إلى مثال المختبر مفتوح الاســتخدام، فبمجرد الانتهاء مــن تحليل أول جهاز حاســب آلي يكون بالإمكان مســح البرمجيات وإعادة تثبيتها من جديد. وهذه هي نقطة الاســترداد والتــي يتم فيها إرجاع جهاز الحاســب الآلي إلى المالك لاســتخدامه في العمليات العاديــة. وإذا تضمنت هــذه الحالة اختبار جهاز أحد أعضاء هيئــة التدريس، فقد ينظر فريق الاستجابة للحوادث الأمنية في الحصول على نسخة من القرص الصلب ومن ثم مسح جميع ما في الجهاز، والتأكد من عمل نسخة احتياطية للبيانات، ومن ثم إعادة تثبيت نظام التشــغيل. وعن طريق الحصول على نســخة من القرص، يكون بالإمكان اســترداد الجهاز بسرعة دون المساس بمهام المستخدم النهائي في حين أن فترة التحليل تستمر.

وبالنظــر إلى مثال آخــر أكثر أهمية، ففي أثناء التحليل إذا اكتشــف فريق الاســتجابة للحــوادث الأمنية أن الباب الخفي مُفعل ويتم اســتخدامه لنقــل (معلومات تحدد الهوية الشــخصية) من خادم مُخــترق إلى مضيف خارج الحرم الجامعــي، فعند ذلك ينبغي قطع الاتصــال في أقــرب وقت ممكن. وبعد ذلك يمكن التعامل مــع الباب الخفي إما من خلال قوائــم التحكم في الوصول للشــبكة أو الجُدر النارية أو الإزالــة الفعلية للباب الخفي من الخــادم، وذلك قبــل التحليل. وفي جميع الحالات فإن أولويــة خصوصية الأصول وتكاملها وجاهزيتها يجب أن تأتي قبل احتياجات المحللين.

يجب أن يكون فريق الاســتجابة للحوادث الأمنيــة على حذر من تأثير التعامل مع أحد الأصول المشــاركة في الحوادث الســلبية. وهنا نذكر موقف يتم فيه تغيير القرارات بشكل جذري كلما توفرت البيانات للتحليل.

الساعة ١:٠٠ بعد الظهر: تم العثور على باب خفي في أحد أجهزة الحاسب الآلي في كلية الطب.

أثناء التحليل، لا بد أن تتبادر بعض الأمور إلى الذهن على الفور. فكلية الطب هي أحد الكليات التــي لديهــا متطلبات للامتثال لـ (قانــون إمكانية نقل التأمين الصحي والمســاءلة) (HIPPA) المرتبــط بالبيانــات. وعليك التأكد سريعــاً مما إذا كان الجهاز يحتوي عــلى بيانات ذات علاقة بقانون (HIPPA). وإذا كان الجهاز يحتوي على تلك البيانات وجب التعامل معها على الفور.

الســاعة ١:١٠ بعد الظهر: لا يحتوي الجهاز على بيانات ذات علاقة بقانون (HIPPA)، ويتبع الجهاز لعضو هيئة تدريس في قسم الطب الإشعاعي خارج منطقة (HIPPA).

بعد مكالمة هاتفية سريعة إلى المسؤول الداخلي تبين أن الجهاز لا يحتوي على بيانات ذات علاقة بقانون (HIPPA). ويمكن لفريق الاستجابة للحوادث الأمنية الانتقال للعمل إذا لزم الأمر. ما هي أنشطة التهديد الذي يشكلها هذا الجهاز؟

الســاعة ١:٣٠ بعد الظهر: تم معرفة أن جهاز الحاســب الآلي جزء من مشروع حصول الجامعة على منحة تُقدر بـ ١٠٠ مليون دولار.

وهنا يُلاحظ اهتمام عميد الكلية ومدير الجامعة، لذا من الأفضل الجدية في النســخ الاحتياطي للجهاز قبل أن تتعرض محتوياته لأي خطر موجه عن بعد.

وقــد يصعب التعافي من بعض الأنشــطة التــي يتم تنفيذها من قبل فريق الاســتجابة للحوادث الأمنية أثناء مرحلة الاحتواء. فالأنشــطة التــي يتم تنفيذها لاحتواء حالة معينة قد تُعرض الجوانب الأخرى من المنظمة للخطر. مثلاً إعادة تشــغيل أنظمة الموارد البشرية لإنهاء إزالة البرمجيات الخبيثة قد تُقاطع عملية تجهيز كشوف الرواتب إذا تم إجراء عملية إعادة التشــغيل في التوقيت الخاطئ. ولهذه الأســباب، ولأقصى حد ممكن، من المهم إبلاغ جميــع الأطــراف المعنية قبل إجراء التغيــيرات اللازمة لعملية احتــواء الأصول. كما يجب اســتمرار أعضاء فريق الاســتجابة للحــوادث الأمنية لمراقبة مبدأ «معرفة مــا نحتاج إليه» أثناء تلك الإبلاغات. فقد يكون من الضروري توضيح أســباب إعادة تشــغيل الخادم لمدير الرواتب، لكن ليس من الضروري توضيح تلك الأسباب لكل شخص في إدارة الرواتب.

ونقطــة أخــرى تحتاج إلى نظر في مرحلــة الاحتواء تتعلق باتخاذ قــرار بخصوص الجلوس ومراقبة ســلوك قراصنة الحاســب أو احتواء المشــكلة على الفور. وكل ذلك يتلخص في كمية الضرر المحتمل على الأصول. ففي حين أن ردة الفعل الأولى لمسؤولي النظام هي التخلص من الخلل وإزالة جميع المسارات، إلا أن مراقبة سلوك قراصنة الحاسب قد تكون مفيدة للمنظمة. فقد تكشــف مراقبة قراصنة الحاســب عن هجمات أخرى موجهة من قبلهم، أو تكشف عن أصول تحت سيطرتهم، كما يمكن أن تكشف عن العديد من المعلومات المفيدة الأخرى.

ويجــب على أعضاء فريق الاســتجابة للحوادث الأمنيــة أن يكونوا على حذر عند اتخاذ قرار بشأن احتواء المشكلة على الفور. فلا بد من تنسيق الجهود قدر الإمكان للقيام بذلك، فمن المعروف أن قرصان الحاسب يتحول إلى قوة مدمرة إذا عرف أنه تم اكتشافه، وذلك في محاولة لتغطية آثاره وإزالة جميع معلومات التسجيل المحلية التي قد تؤدي للقبض عليه. وقد يقوم مسؤول قاعدة البيانات المتورط في حالات الاحتيال بنصب الفخاخ التي تؤدي إلى تدمير قاعدة البيانات وكافة البيانات الواردة فيها.

ولهــذا الســبب يقوم عملاء مكتب التحقيق الفيدرالي (FBI) عنــد القيام بعمليات القبض على قراصنة الحاســب بإبعادهم بسرعــة وبكل قوة عن لوحة المفاتيح وأجهــزة الإدخال الأخرى في أقــرب وقت ممكن. وهذا يقلل من احتمالية مبادرتهم بإنشــاء نصوص برمجية لتدمير الأصول وتدمير الأدلة التي تُدينهم.

الدروس المستفادة:

المرحلــة النهائيــة من إجــراءات التعامل مع الحــادث الأمني هي ما يســمح للتحضير للحــادث القادم. وفي هــذا الجزء الأخير يقــوم أعضاء فريق الاســتجابة للحوادث الأمنية بتجميع ملاحظاتهم واستكمال عملية التوثيق. وينبغي أن يتضمن التوثيق جميع الأحداث الســلبية الفردية مع تحديد وقت الحادث الأمني والأصول المعنية. كما يتضمن التوثيق ما يلي:

- الإشارة إلى جوانب المنظمة التي تأثرت بالحادث وتحديد نتيجة الاختراق.
- كيــف تعاملــت كل إدارة منفردة مع التهديــدات الأمنية؟ وكيــف تعاملت تلك الإدارات مجتمعة تحت تنسيق فريق الاستجابة للحوادث الأمنية؟
- مدى مناسبة الإجراءات الحالية للتعامل مع الحوادث، وتحديد فرص التحسين.
- مدى مناسبة تحديد وتصنيف الأصول وأثر ذلك في اتخاذ فريق الاستجابة للحوادث الأمنية لقرارات سريعة تناسب تطور الحالة.
- مدى مشاركة المعلومات مع المستفيدين ومدى الرضا عن ذلك.
- فرص الكشف الاستباقية لتجنب حدوث مشكلات مشابهة.
- التدابير التقنية اللازمة التي يجب اتخاذها لتجنب قضايا مماثلة في المستقبل.

إذاً كيف تم حل مشكلة إدارة التنمية الاقتصادية (EDA) في نهاية المطاف؟

في شهر فبراير من عام ٢٠١٣، أي بعد أكثر من عام على التنبيه الأولي، أكد مكتب المفتش العام في وزارة التجـارة لكل مـن إدارة التنمية الاقتصادية ووزارة التجـارة أن الأضرار اقتصرت فقط عـلى نظامين. وبعد تأكد وزارة التجارة من عدم وجود حادث كبير، بدأت وزارة التجارة بجهود الاسـترداد في شـهر فبراير من عام ٢٠١٣، واحتاجت لفترة أطول من ٥ أسـابيع بقليل لاستعادة القدرات التشغيلية السابقة لإدارة التنمية الاقتصادية.

وبمقارنـة الفترات الزمنية نجد جهود إدارة التنمية الاقتصادية الناقصة قد امتدت لما يقارب من العام.

وبالتحديد قامت وزارة التجارة بتزويد إدارة التنمية الاقتصادية بخدمات إدارة حسـابات البريد الإلكـتروني للمنظمة، وخدمات مكتب الدعم الفني، كما قامت بتهيئة آمنة لنسـخ موحدة من أقراص أجهزة الحاسب المحمولة.

بالإضافـة إلى ذلك قامت الإدارة بإعادة وصول مسـتخدمي إدارة التنمية الاقتصادية لتطبيقات الأعمال الهامة.

الكارثة:

في عـالم الحوادث هناك أمـرٌ مخيف يؤثر تأثيراً ضخماً في جميـع أنحاء المنظمة والذي يستطيع إخضاع الشركة المزدهرة على ركبتيها، وهذا الأمر المخيف هو الكارثة. والكارثة هي حادثة مفجعة تتسـبب في دمار كبير. ويمكن اعتبـار الكارثة بأنها حادث ضخم، أو حادث كبـير ينطوي على حوادث فرعية متعددة، أو حادث يؤثـر في المنظمة بأكملها. وأياً كانت الطريقة التي تنظر بها إلى الكارثة، فإن لها آثاراً كبيرة على العديد من المستفيدين.

ونبـدأ هذا القسـم ببعض التعاريف: التعافي من الكوارث هـي العملية التي تقوم بها منظمة تقنية المعلومات من أجل إعادة الأنظمة الاحتياطية وتشغيلها. والتعافي من الكوارث قد يشمل انتقال العمليات إلى موقع آخر بهدف استرداد الخدمات والبيانات.

في عام ٢٠٠٢، حدث فشل في أجهزة خوادم البريد الإلكتروني الخاص بالطلاب مما أدى إلى فقدان ٣٠ ألــف حســاب بريد إلكتروني للطلاب في جامعة جنوب فلوريدا بمــا في ذلك البيانات الواردة في حســابات البريد الإلكتروني. وعلى الفور بدأ العمل بخطة التعافي من الكوارث والتي تتضمن إعادة إنشــاء جميع حســابات البريد الإلكتروني للطلاب. وهذه الحســابات ســتكون فارغة في البداية لكنها ستســمح للطلاب بإرسال واستقبال رســائل البريد الإلكتروني. وبمجرد الانتهاء من هذه الخطوة، ســيتم استخراج بيانات البريد الإلكتروني من الشريط الاحتياطي ومن ثم إعادتها إلى صناديق البريد الإلكتروني الخاص بالطلاب. وقد استغرقت عملية التعافي من الكارثة بأكملها في هذه الحالة قرابة ٣ أسابيع.

والتعــافي من الكوارث عملية معقدة للغاية، ويتــم معالجتها عادة من قبل أفراد ذوي خــبرة طويلة في المنظمة. وفي المنظمات الكبيرة غالباً مــا يكون هناك أفراد مخصصين لهذا الموضوع. وفي جميع الحالات فإنه ليس من المرجح أن توكل إليك مســؤوليات التعافي من الكــوارث في وقت مبكر من حياتك المهنية، لذا فإن هــذا الموضوع لن يتم تغطيته في هذا الكتاب. وقد تطرقنا لهذا الموضوع بهدف تعريفك ببعض المفاهيم الأساســية حتى تتمكن من المساهمة في هذه العملية.

ويُعد التعافي من الحوادث جزءاً من الصورة الأكبر وهي التخطيط لاســتمرارية الأعمال (Business Continuity Planning) أو اختصاراً (BCP). والتخطيط لاستمرارية الأعمال هــو عملية الحفــاظ على عمليــات المنظمة في الظروف العســيرة. ففي أثنــاء التخطيط لاستمرارية الأعمال، يتوقع المخططون ما سيحدث في حال وقوع كارثة، وعليه يحددون الحد الأدنى والضروري لمساعدة المنظمة في استمرار عملياتها. وفي حالة نظام البريد الإلكتروني في جامعة جنوب فلوريدا، تشــمل الأسئلة ما يلي: كيف سيُسلِم الطلاب واجباتهم؟ ومن أين سنأتي بالتمويل اللازم لشراء الأجهزة الجديدة؟ وكيف سنقوم بمطالبات التأمين؟ وما الآثار الأخرى التي سيسببها انقطاع البريد الإلكتروني عن المنظمة؟

وبحكم طبيعة التخطيط لاستمرارية الأعمال والتعافي من الكوارث فإنها تشمل وحدات أخــرى بالإضافــة إلى وحــدة تقنية المعلومات. على ســبيل المثال، ليــس منطقياً أن تعمل المنظمة معزولة بعضها عن بعض عند الاستعداد لإعصار أو عاصفة. إن مثل هذه الحوادث

ســتؤثر في المنظمة بأكملها. فالموارد البشريــة قد تتطلب بقاء جميع الأفراد في منازلهم إذا كان هناك احتمال لإعصار من المســتوى الرابع أو أعلى. وفي الوقت نفسه قد تحتاج وحدة تقنية المعلومات إلى حضور الموظفين لإيقاف تشغيل الخوادم والأجهزة الحاسوبية المكتبية. لذا فإن التنسيق بين هذه المجموعات سوف يضمن تنفيذ الإجراءات المناسبة.

وجزء مهم من التخطيط لاستمرارية الأعمال هو تحليل تأثير العمل (Business Impact Analysis) أو اختصاراً (BIA). وتحليل تأثير العمل هو تحديد الخدمات والمنتجات البالغة الأهميــة للمنظمة. وهنــا يأتي دور تصنيف الأصول الذي تعرضنا له في الفصول الســابقة. وبناءً على ذلك فإن الأصول الضرورية هي تلك الأصول التي تدعم الخدمات والمنتجات ذات العلاقــة بتحليل التأثير على العمل. وبعد ذلــك يحدد (تحليل التأثير على العمل) أولويات إجراءات التعافي من الكوارث.

والهدف الأســاسي للتخطيط لاســتمرارية الأعــمال والتعافي من الكــوارث هو الحفاظ عــلى أمــن الموظفين وعائلاتهم حيث يجب ألا يوضع الموظــف في خطر. كما يجب أن يتم الاســتعداد للسماح بتطبيق إجراءات استعادة الأصول التي لا تتضمن حالات خطرة. وهنا بعض الأمور الأخرى التي يجب الاهتمام بها:

- قائمة بأرقام الهواتف وهي أداة مفيدة للغاية في حال وقوع كارثة. ربما قائمة بسيطة بحجم البطاقة وتحتوي على أرقام الهواتف تكون لدى الموظفين.
- كيف ستخبر زملاءك الموظفين في حال تعطل أنظمة الهاتف؟
- إذا قمت بنسخ ملفاتك الاحتياطية داخلياً في شريط وبواسطة جهاز مرفق مع الخادم، كيف ستقوم بنسخ البيانات في موقع آخر؟ وما البيانات التي يجب استعادتها أولاً؟
- هل هناك شخص آخر يعرف كيفية استعادة البيانات؟ هل يوجد تعليمات منشورة في مكان ما؟ وإذا كان من المتوقع أن يقوم الشــخص بقراءة كُتيب من ١٠٠ صفحة للبدء في استعادة البيانات، عندها يجب أن يتم البدء في تبسيط الإجراءات.
- هل يتم اختبار استعادة النظام بشكل دوري؟ الأشرطة والوسائل الأخرى قد تهترئ، أو تُخدش، ومن ثم تصبح غير قابلة للقراءة.

• هل هناك وسـيلة للحصول على أجهزة جديـدة لتحل بسرعة محل الأجهزة القديمة التـي تضررت بسـبب الكارثـة؟ وإذا كان يوجـد تأمين على الشـبكات والأجهزة الحاسوبية، من هو الموظف الذي يعرف تفاصيل تفعيل التأمين؟

نموذج حالة - قرصنة في الحرم الجامعي:

> هذه الملاحظات الشـخصية لمسـؤول النظام حـول إحدى الحالات في جامعـة جنوب فلوريدا. وحدثت هذه الحالة قبل عام ٢٠٠٥ وتم تغيير أسماء جميع الشخصيات وأسماء المضيف وذلك لحمايـة الأفراد المعنيين. ومـن الصعب العثور على تقارير الحوادث التفصيلية المشـابهة لهذا التقرير وذلك لأنها تتعلق بمبدأ «معرفة ما نحتاجه» ولا يتم نشرها مطلقاً.

سوف نُسمي الطلاب (Greg Apple) و (John Orange). وتخصصات هذين الطالبين غير معلنة. وفيما يلي نستعرض ملاحظات مسؤول النظام حول الجدول الزمني للحادثة:

يوم الإثنين الموافق ١٧ أكتوبر:

تلقيت تقارير تفيد بأن قسـم الجذر في خـادم (SERVER-A) كان ممتلئاً. واتضح أن اثنين من الطلاب (أسـماء الدخول على النظام هي jorange وgapple) يستخدمون الدليل الفرعـي (/tmp) لحفظ ملفات مضغوطة حجمها ١٠ جيجا بايت. لذا قمت بإزالة معظم الملفات.

وفي المساء تلقيت البريد الإلكتروني التالي من مسؤول الشبكة:

«أنا مشـوش الليلة بسبب حساب يحمل الاسم (gapple) على خادم (SERVER-A)... قام هذا الحساب بتسجيل الدخول مرتين في نفس الوقت ومن مناطق مختلفة من البلاد... وعـلاوة على ذلك يبدو أن هذا الشـخص قد حصل على ملف كلـمات المرور، والموجود في حسـابه، من مكان ما على الشبكة...ويبدو أن هذا الشخص لا ينام مطلقاً...سأتحدث معك حول هذا الموضوع في الصباح...».

ويبدو أن ملف كلمات المرور صدر من موقع (somedomain.com).

ويحتــوي كلٌّ من ملف كلمات المرور وحســاب (gapple) على قائمــة أدلة طويلة من المســتخدم (mikel). وقمت بالبحث عن (mikel@somedomain.com) وقد تم العثور عليه، كما قمت بإرســال بريد إلكــتروني إلى (root@somedomain.com) لكن لم أحصل على أي رد.

يوم الثلاثاء الموافق ١٨ أكتوبر:

لاحظت في الصباح عند تسجيل الدخول إلى خادم (SERVER-A) أن حساب (jorange) متصل بـــ (somedomain.com) عبر بروتوكول (telnet). وقــررت عندها فحص الدليل الرئيسي لحساب (jorange) ووجدت أن تصميم الدليل الرئيسي يشابه إلى حد بعيد الدليل الرئيسي لحساب (gapple).

ثم اســتخدمت بروتوكول نقل الملفات (FTP) لنقل بعــض الملفات المحفوظة في دليل (/tmp) إلى جهــازي المكتبي وقمت بفك الضغــط عنها. واتضح أن تلك الملفات عبارة عن ألعاب إلكترونية مقرصنة. وبعد ذلك بدأت بمراقبة أنشــطة حساب (jorange) عن كثب. نشطاً

أخبرني (Will) وهو مســؤول الشــبكة أن موقع (thepoint.com) هو موقع شــبكات مجــاني مزود بروابط إنترنت متكاملة مــع إمكانية الوصول إلى القشرة (shell). كما أخبرني بأن لديه حساباً في ذلك الموقع. وبما أني لم أتلق أي رد من (root@thepoint)، طلبت من (Will) أن يقــوم بتســجيل الدخول لمعرفة إمكانية التحري عــن دليل (mikel). وقد عثر (Will) على ثلاثة ملفات لكلمات المرور، كما عثر على المزيد من الألعاب الإلكترونية.

****

من ملفات السجل عثرت على الروابط التالية وهي إما لحساب (gapple) أو لحساب (jorange):

(numsix@inca.anotherdomain.net) - حساب (Jack Laughlin)

(hopi.anotherdomain.net)

(mikel@somedomain.com) - حساب (Mike Lee)

(thriddomain.net.server٠) - حساب (Randy Sharr)

وقد يكون هناك المزيد من الحسابات المخترقة على هذه المواقع.

****

الأدلة على حساب (gapple):

١. ملف كلمات المرور من موقع (somedomain.com).

٢. ملف يحتوي على قائمة من الدليل التالي (thepoin.com:/~mikel).

٣. ملفات السجل تشير إلى تسجيل الدخول من (gapple@servera) إلى (jorange@servera).

الأدلة على حساب (jorange):

١. البرمجيات المقرصنة والموجودة في (/tmp). ولدينا نُسخ من البرمجيات على خادم محلي آخر لكن الملفات الفعلية تمت إزالتها ليلة أمس وذلك قبل إغلاق الحساب.

٢. الرسائل الإلكترونية التي تلقاها حساب (jorange) من مستخدمين مجهولين بخصوص موقع جديد للبرمجيات المقرصنة، وتم تأكيد وجود هذا الموقع الجديد.

٣. ملفات السجل الخاصة باستخدام بروتوكول نقل الملفات (FTP) من موقع (somedomain.com) باستخدام حساب وهمي لـ (mikel). تم تأكيد وجود حساب (mikel@somedomain.com) وجميع محتوياته من البرمجيات المقرصنة بواسطة (root@somedomain.com).

ونتيجة لذلك تم إيقاف كلا الطالبين عن الدراسة الجامعية وذلك لتجاوزهم قواعد السلوك الأخلاقي (Code of Ethics).

الملخص:

ناقشنا في هذا الفصل عملية التعامل مع الحوادث الأمنية. ورأينا أن المنظمات الفعالة لا تنتظر وقوع الحوادث الأمنية قبل معرفة كيفية التعامل معها. وبدلاً من ذلك تقوم المنظمات بالاستعداد الاستباقي للتعامل مع حوادث أمن المعلومات. وهذا الاستعداد يتطلب إعداد سياسة لتوجيه الاستجابة للحوادث، واتفاقيات خطط التواصل، وإجراءات تأسيس فريق الاستجابة للحوادث الأمنية، والحصول على الأدوات المناسبة للاستجابة للحوادث. ويتم اكتشاف الحوادث عن طريق السلوكيات غير الطبيعية. ولقد رأينا أنه أثناء

الاســتجابة للحوادث الأمنية قد يُصبح من الضروري تعطيل الخدمات وذلك لاحتواء الضرر. وأخيراً استعرضنا المفاهيم المتصلة بالكوارث أو الحوادث ذات النطاق الواسع.

أسئلة مراجعة للفصل:

١. ما حوادث أمن المعلومات؟

٢. اذكر بعض الأمثلة على الحوادث الأمنية، ويُفضل أن تكون عايشت الأمثلة بنفسك.

٣. ما الخطوات الأساسية للتعامل مع الحوادث الأمنية؟

٤. في خطوات التعامل مع الحوادث الأمنية أعلاه، ما أهم خطوة في رأيك؟ ولماذا؟

٥. ما الأنشطة الهامة ذات العلاقة بالإعداد للتعامل مع للحوادث الأمنية؟

٦. ما سياسة الاستجابة للحوادث الأمنية؟ وما أهميتها؟

٧. ألق نظرة على إحدى سياسات الاستجابة للحوادث الأمنية لأحدى المنظمات (ويمكن العثور عليها بســهولة من الإنترنت). ما عناصر هذه السياسة؟ في اعتقادك ما المثير للاهتمام في هذه السياسة؟

٨. ما نطاق سياسة أمن المعلومات؟ وما أهمية تحديد هذا النطاق؟

٩. ما فريق الاستجابة للحوادث الأمنية؟ وكيف يتم تشكيله؟

١٠.ما هي بعض القضايا المتعلقة بالتواصل بخصوص التعامل مع الحوادث الأمنية؟

١١.ما مبدأ «معرفة ما نحتاج إليه»؟ وما فائدته في التعامل مع الحوادث الأمنية؟

١٢.ما الامتثال؟ وما أهميته للتعامل مع الحوادث الأمنية؟

١٣.كيف يساعد التدريب في التعامل مع الحوادث الأمنية؟

١٤.اختر إحدى شــهادات أمن المعلومات واقــرأ منهجها الدراسي. في جملة واحدة لكل منها، اشرح كيف تساعد ثلاث وحدات من ذلك المنهج الدراسي على تحسين قدراتك في التعامل مع الحوادث الأمنية.

١٥.ما الطرق الشائعة في اكتشاف الحوادث الأمنية؟

١٦.ما تحليل السجل؟ وما استخداماته؟

١٧.إذا كنت تستخدم أداة لمراقبة سلامة الملفات مثل (OSSEC) في جهاز الحاسب الآلي الخاص بك، ما المجلدات المناسبة للمراقبة باستخدام تلك الأداة؟ ولماذا؟ (قد ترغب في تجربة احدى الأدوات المفتوحة المصدر مثل (OSSEC)).

١٨.ما أهداف تحليل الحوادث الأمنية؟

١٩.مـــا الاحتواء؟ وما أهميته؟ وما هي بعض التدابير التي يمكن اتخاذها لاحتواء ضرر هجمات الفيروسات؟

٢٠.ما الاستئصال؟ وما هي بعض التدابير التي يمكن اتخاذها لاستئصال هجمات الفيروسات؟

٢١.كيف يساعد التعامل مع الحوادث الأمنية على تحسين أمن المعلومات للمنظمة في المستقبل؟

٢٢.افترض أنّك تُعد الفصل الدراسي السابق احدى الحوادث التي مرت عليك. اكتب فقرة مبســطة عن «الدروس المستفادة» وذلك باتباع نموذج مماثل للنموذج المستخدم في التعامل مع الحوادث الأمنية. قم بتعميم الدروس المســتفادة بشــكل مناسب دون تحديد أسماء الشخصيات، وذلك للمحافظة على خصوصيتك.

٢٣.ما الكارثة؟ وما التعافي من الكوارث؟

٢٤.ما التخطيط لاستمرارية الأعمال؟ وما هي بعض الأشياء التي يمكنك القيام بها كجزء من ممارسة التخطيط لاستمرارية أعمال بياناتك الشخصية؟

٢٥.ما تحليل التأثير على العمل؟ وكيف يكون هذا التحليل مفيداً؟

أسئلة على نموذج الحالة:

١. من بين آليات الكشــف عن الحوادث التي تم وصفها في هذا الفصل، ما الآلية التي أدت إلى الكشف عن الحادث؟

٢. من الأشخاص المناسبين في الحرم الجامعي ليتم إخطارهم بالحادث حال اكتشافه؟

٣. ما الدروس التي تعلمتها من قراءتك عن الحوادث الأمنية؟

نشاط التدريب العملي - الجدول الزمني للحوادث الأمنية باستخدام (OSSEC):

في هذا التمرين سوف نستخدم برنامج (OSSEC) الذي تم تثبيته خلال التدريب العملي في الفصل التاسع وذلك لمراقبة حادث مصطنع وبناء جدول زمني لهذا لحادث.

ولبدء محاكاة الحادث، انتقل إلى حساب المستخدم ذو الصلاحيات العليا وقم بتنفيذ البرنامج النصي الخاص بالمحاكاة:

```
[alice@sunshine ~]$ su -
Password: thisisasecret

[root@sunshine   &tilde;]#  /opt/book/
incident-handling/scripts/begin_incident

#######################################
#########################

Simulated Incident has begun!
This script will run for 10- 20 minutes.

#######################################
#########################
```

وبمجرد انتهاء البرنامج النصي، قم بتشغيل واجهة (OSSEC-WebUI) عن طريق فتح متصفح الإنترنت وزيارة موقع (http://sunshine.edu/ossec).

أسئلة:

١. كيف حاول المهاجم الوصول إلى النظام؟ وما الحساب الذي كان يستهدفه؟

٢. عند الانتهاء من اختراق الحساب، هل هناك حسابات أخرى تم اختراقها؟

٣. هل تم تثبيت برمجيات جديدة؟

٤. هل تم فتح أو إغلاق منافذ شبكة جديدة؟

٥. هل تم إضافة أي حسابات جديدة إلى النظام؟

٦. قم بإنشـاء جدول زمني للأحداث الرئيسـية في هذا الحادث. ويمكن تحميل نموذج الجـدول الزمنـي من نماذج مايكروسـوفت وورد (MS Word) عـلى الرابط التالي (http://office.microsoft.com/en-us/templates/timeline-TC001016265.aspx)

تمرين التفكير النقدي - الهدم في إدارة التنمية الاقتصادية:

يعد تقريـر إدارة التنمية الاقتصادية مفيداً جداً لكل مهتـم بالتعامل مع حوادث أمن المعلومات. ولمزيد من التفكير، نذكر هنا مقتطفات أخرى من التقرير:

عـلى الرغم من توصيات التعافي الصادرة عـن وزارة الأمن الداخلي (DHS) وعن وكالة الأمن القومي الأمريكية (NSA) والمتضمنة تقديم المشورة لإدارة التنمية الاقتصادية بالتركيز على اسـترداد أنظمة تقنية المعلومات بسرعة وبشكل كامل، ركزت إدارة التنمية الاقتصادية بدلاً عـن ذلك على بناء بنية تحتية جديدة لتقنية المعلومات كما ركزت على إعادة تصميم تطبيقات الأعمال. وفي شـهر سـبتمبر من عام ٢٠١٢ (أي بعد ٨ أشـهر من عملية العزل) تقدمـت قيادة إدارة التنمية الاقتصاديـة بطلب لمجلس مراجعة تقنية المعلومات التجارية (Commerce IT Review Board) لإعـادة برمجة الأمـوال اللازمة لتنفيذ جهود التعافي، لكن المجلس لم يوافق على طلب إدارة التنمية الاقتصادية. وقدّرت إدارة التنمية الاقتصادية أنها ستحتاج إلى أكثر من ٢٦ مليون دولار للإنفاق خلال الثلاث سنوات القادمة (زيادة من ٣,٦ مليـون دولار إلى مـا يقرب مـن ٨,٨٣ مليون دولار أي أكثر من ٢,٥ مرة من متوسـط الميزانية السنوية لتقنية المعلومات التابعة للإدارة) وذلك لتمويل جهود التعافي.

لذا سيقوم المشكّكون في موضوعات الحكومة الكبيرة باستخدام هذه المعلومات الواردة في تقرير مكتب المفتش العام للإشـارة إلى أن إدارة التنمية الاقتصادية استخدمت الحادث

الأمنـــي كذريعة لتدمير بنية تقنية المعلومات حتى تتمكن من تأمين التمويل اللازم لأجهزة تكنولوجيـــة جديدة، أو بمعنى آخر محاولة طلاء بنيتها التحتية بالذهب. كيف ســتؤيد أو ستعارض هذه الفكرة بناءً على المعلومات الواردة في هذا التقرير؟

تصميم حالة:

طلــب منك مدير الجامعة إعداد وثيقة من صفحــة واحدة توضح فيها الخطوات التي ســتتخذها لإنشــاء فريق الاســتجابة للحوادث الأمنية، ولتوضيح كيفيــة الإعداد لهجمات القرصنة. وبعد قيام مورد تأمين الشــبكات بتقديم ســيناريو مقنع عن الدمار والكآبة التي قد تحدث بســبب الهجمات، أصبــح رئيس الجامعة ومديرها قلقــيْنَ بخصوص عدم قدرة الجامعة على التصرف بسرعة وبشــكل حاسم لحل أي مشكلة قد تحدث، وهذا سوف يؤثر في صورة الجامعة.

وفي التقرير المطلوب منك، أجب عن الأسئلة التالية:

١. ما النقاط التي يجب الاهتمام بها في سياسة الاستجابة للحوادث؟

٢. مــا الوحدات التي ينبغي أن يكون لها تمثيل في فريق الاســتجابة للحوادث الأمنية؟ علل إجابتك.

٣. ناقش مركزية الموارد المتعلقة بأمن الحرم الجامعي.

٤. قم بالبحث اللازم لتحديد متطلبات الإبلاغ في ولايتك في حال حدوث اختراق.

٥. قم بالبحث اللازم لمعرفة الحماية التي يوفرها تأمين أمن الشبكات.

الفصل الثاني عشر

تحليل الحوادث الأمنية

نظرة عامة:

في الفصل الســابق ألقينا نظرة عامــة على عملية التعامل مع الحــوادث الأمنية حيث ناقشنا المراحل المختلفة لتلك العملية وهي:

- الإعداد: تجهيز البنية التحتية اللازمة للتعامل مع الحوادث الأمنية عند وقوعها.
- التحليل: اكتشاف وتوثيق أكبر قدر ممكن من الحادث.
- الاحتواء: تحديد أفضل وســيلة لمعالجة وإزالة الآثار المتبقية للحادث وذلك اعتماداً على نتائج التحليل.

الدروس المســتفادة: تطبيق المعرفة الجديدة لإصلاح أي مشــكلات وُجدت خلال هذه العملية، ومن ثم العودة إلى مرحلة الإعداد.

ودورة التعامل مع الحوادث الأمنية لا تنتهي أبداً، فهناك ثغرات جديدة تظهر، وتقنيات جديــدة تُســتخدم، وتحديات جديدة تطفو على الســطح. وإذا كان هناك خلل في مرحلة الإعداد، وهي المرحلة التي تحاول المنظمة أن تكون فيها اســتباقية في التعامل مع الثغرات، فإن ذلك حتماً سيؤدي إلى عواقب سلبية.

وفي هذا الفصل سنُلقي نظرة فاحصة على المرحلتين الثانية والثالثة وهما مرحلة التحليل ومرحلة الاحتواء من خلال:

- النظر إلى مصادر المعلومات في نظام تشغيل لينكس ونظام تشغيل ويندوز.
- معرفة كيفية استخراج المعلومات من تلك الأنظمة وذلك فيما يخص الأحداث التي نستعرضها.
- معرفة كيفية إنشاء جدول زمني يوضح نمط الحادث.
- النظر في أمثلة على أدلة الهجوم وذلك في تطبيقات متعددة.

تحليل السجل:

تحتوي مُعظم التطبيقات البرمجية ونُظم التشـغيل على آلية تدوين لتسجيل معلومات الحالة. وتختلف أغراض تسجيل المهام بناءً على التطبيق.

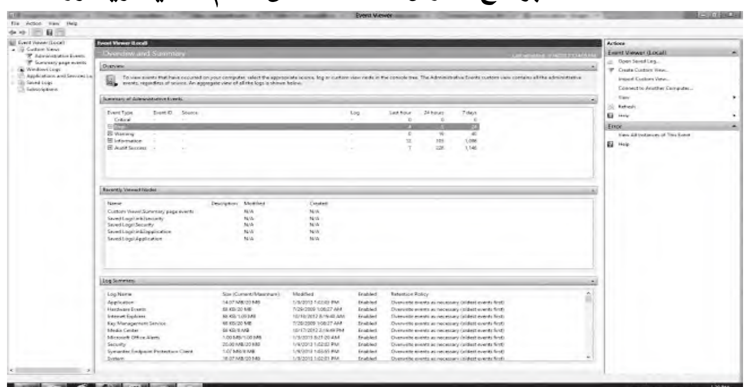
- يستخدم مطورو البرمجيات التسجيل لضمان أن التطبيق يعمل كما هو متوقع. على سبيل المثال، قد يُقرر مطورو البرمجيات إظهار مخرجات أمر داخلي على الشاشة في بعض الحالات، ويعرف هذا عادة بتشغيل التطبيق في وضع التصحيح.
- ويستخدم مسؤولو النظم معلومات التسـجيل للقيام بتحليل الأداء لمعرفة إنتاجية التطبيق. على سـبيل المثال، قد يراقب مسـؤولو النظم السجل للتأكد أن التطبيق لديه ما يكفي من الذاكرة ومن مساحة القرص للعمل بالشكل الصحيح.
- ويسـتخدم مسؤولو الأمن السـجل أثناء مرحلة تحليل الحادث الأمني. وفي الواقع فإنـه مـن المرجح أن يكون الوصول إلى سـجل النظام هو الأمـر الأول الذي يطلبه المسؤول الأمني كجزء من التحقيق.

وفي هذا القسـم سـنُلقي نظرة فاحصة على السجل بشـكل عام بما في ذلك سجل نظام التشغيل وسجل التطبيقات.

سجلات نظام التشغيل ويندوز:

ويعرف سـجل نظام التشغيل ويندوز بـ «سـجل الأحداث». ويوضح الشكل (١٢-١) واجهة ويندوز التي تتيح للمسـتخدم الاطلاع على السـجل. وهذا البرنامج يُعرف باسـم «عـارض الأحـداث» (Event Viewer). وهنـاك أدوات أخرى مفتوحـة المصدر وأدوات تجارية يمكن اسـتخدامها للحصول على معلومات أكثر من ملفات سجل الأحداث في نظام التشـغيل ويندوز. ويمكن الاطلاع على مئات من تلك الأدوات من خلال بحث بسيط على الإنترنت.

الشكل (١٢-١): شاشة برنامج (عارض الأحداث) على نظام تشغيل ويندوز ٨



الجانـــب الأيمن من (عارض الأحداث) هو جانب خاص بالتنقل والذي يتيح للمســؤول الاطلاع على الســجلات المختلفة والموجودة في هذا النظام. وفي هذا الجزء أيضاً يســتطيع المسؤول إنشاء طُرق عرض مخصصة للتركيز على أهداف محددة.

الشاشة الرئيسية لبرنامج عارض الأحداث:

تتكون الشاشة الرئيسية لبرنامج عارض الأحداث، والموضحة في الشكل (١٢-١)، من ثلاثة جوانب كل منها يحتوي على معلومات مختلفة عن ملفات السجل.

ملخــص لجانب الأحداث الإدارية وهــذا الجزء يحتوي على تفصيل لعدد الأحداث بناءً عــلى نوع الحدث. فإذا قام المســؤول بتوســيع نوع الحدث من خــلال النقر على زر (+) الموجود بجانب النوع فإن عدد الأحداث المصنفة تحت نوع معين يتم تقســيمها بواســطة مُعــرِف الحــدث (Event ID). ومُعرفــات الحدث هي تصنيفات تحــت نوع محدد من الأحداث (الشكل ١٢-٢).

الشكل (١٢ -٢): ملخص لجانب الأحداث الإدارية

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour	24 hours	7 days
Critical	-	-	-	0	0	0
⊞ Error	-	-	-	2	15	35
⊞ Warning	-	-	-	5	9	44
⊞ Information	-	-	-	24	627	1,595
⊞ Audit Success	-	-	-	68	223	1,192

جانب ملفات الســجل التي تم عرضها مؤخراً: ويحتوي هذا الجزء على ملفات ســجل الأحــداث التي تم عرضهــا مؤخراً. وفي الواقــع، يحتوي هذا الجانب عــلى وصف للعرض (عندمــا يكون متاحاً)، وتاريخ آخر تعديل لملف الســجل (بمعنى آخر، متى تمت الكتابة في هذا الملف)، ومتى تم إنشــاء الملف في الأصل. وتُشير سطور التواريخ الفارغة إلى أن الملف لم يتم إنشاؤه أصلاً أو إلى أن مُدخلات السجل لم يتم إلحاقها بالملف (شكل ١٢-٣).

الشكل (١٢-٣): ملفات السجل التي تم عرضها مؤخراً

Recently Viewed Nodes

Name	Description	Modified	Created
Custom Views\Summary...		N/A	N/A
Windows Logs\System	N/A	1/14/2013 3:29:13 PM	7/29/2009 1:05:19 AM
Windows Logs\Applicati...	N/A	1/14/2013 3:29:14 PM	7/29/2009 1:05:19 AM
Windows Logs\Forwarde...	N/A		
Windows Logs\Setup	N/A	12/20/2012 8:09:35 AM	7/29/2009 1:08:23 AM
Windows Logs\Security	N/A	1/14/2013 3:29:13 PM	7/29/2009 1:05:19 AM
Custom Views\Administr...	Critical, Er...	N/A	N/A
Saved Logs\inb2security		N/A	N/A
Saved Logs\Security		N/A	N/A

ملخص السجل:

الجانب الأخير في الشاشــة الرئيسية لبرنامج عارض الأحداث هو جانب ملخص السجل. ويقوم هذا الجانب بوصف خصائص ملفات السجل التي يحتفظ بها نظام التشغيل ويندوز حالياً. أما عمود (Size/Maximum) فيُخبر المسؤول عن حجم المساحة المتبقية والمسموحة للزيادة في ملف السجل. وإذا رأيت أن حجم ملف السجل وصل للحد الأقصى أو اقترب من ذلك فمن المرجح أن الســجلات المحفوظة في تلــك الملفات تكون في حالة تدوير مما يؤدي إلى فقدانها (الشــكل ١٢-٤). وهذا يطرح السؤال: كم عدد ملفات السجلات اليومية التي يستطيع الجهاز الاحتفاظ بها دون فقدان؟

وســتلاحظ أن ســجل الأمن يمتلئ عادة بسرعة مما يتطلب التدوير في معظم الحالات أكثر من السجلات الأخرى. وهذا ينطبق بشكل خاص على خوادم الويندوز. واعتماداً على عدد مستخدمي الخادم، فإن استخراج معلومات مفيدة من ملفات سجل الأمن قد يكون عديم الفائدة.

لاحظ أيضاً وجود عمودَين آخرين في جانب ملخص السجل. من خلال هذين العمودين يمكنــك تأكيد مــا إذا تم تمكين خدمة ســجل معينة، كــما يمكنك معرفة مــا إذا تم تعيين خدمة الكتابة فوق المعلومات الحالية عندما يكون ملف الســجل ممتلئاً أو خدمة تجاهل المدخلات الجديدة عندما يكون ملف السجل ممتلئاً.

الشكل (١٢-٤): جانب ملخص السجل

Log Summary

Log Name	Size (Current/Maximum)	Modified	Enabled	Retention Policy
Application	14.07 MB/20 MB	1/14/2013 3:29:14 PM	Enabled	Overwrite events as nec...
Hardware Events	68 KB/20 MB	7/29/2009 1:08:27 AM	Enabled	Overwrite events as nec...
Internet Explorer	68 KB/1.00 MB	10/18/2012 8:19:40 AM	Enabled	Overwrite events as nec...
Key Management Service	68 KB/20 MB	7/29/2009 1:08:27 AM	Enabled	Overwrite events as nec...
Media Center	68 KB/8 MB	10/17/2012 2:19:49 PM	Enabled	Overwrite events as nec...
Microsoft Office Alerts	1.00 MB/1.00 MB	1/14/2013 3:26:01 PM	Enabled	Overwrite events as nec...
Security	20.00 MB/20 MB	1/14/2013 3:29:13 PM	Enabled	Overwrite events as nec...
Symantec Endpoint Prot...	1.07 MB/8 MB	1/14/2013 3:30:56 PM	Enabled	Overwrite events as nec...
System	18.07 MB/20 MB	1/14/2013 3:29:13 PM	Enabled	Overwrite events as nec...

أنواع ملفات سجل الأحداث:

بعض ملفات سـجل الأحداث موجودة في أنظمة تشـغيل وينـدوز منذ إصدار ويندوز إكس بي (XP). وبإمكانك الاطلاع على ملفات سـجل ويندوز في الجانب الأيسر من الشكل (١٢-٢).

- يحتوي سـجل التطبيقات على معلومات التسـجيل من تطبيقـات الطرف الثالث، ولا تُعد تطبيقات مايكروسـوفت جزءاً من التوزيع الأسـاسي لنظام التشغيل. على سـبيل المثال، معلومات تسـجيل الألعـاب الإلكترونية، ومعلومات تسـجيل برامج مايكروسوفت أوفيس تكون في ملف سجل الأحداث التابع للتطبيقات.
- ويعد ملف الأمن إلى حد كبير مستودعاً افتراضياً لمحاولات تسجيل الدخول والخروج. ويمكن تعديل تهيئة هذا الملف حتى يمكنه تسجيل إنشاء ملفات البيانات أو إغلاقها أو فتحها داخل النظام.
- يحتوي ملف سجل الأحداث الخاص بالنظام على رسائل سجل نظام التشغيل. على سبيل المثال، يتم تسجيل مشكلات الاتصال بالشبكة، وأخطاء مشغل بطاقة الفيديو في ملف سجل أحداث النظام.

ويحتوي نظام التشغيل ويندوز ٨ على نوعين إضافيين من ملفات سجل الأحداث:

١. ملف سـجل الأحداث الخاص بالإعـداد والذي يحفظ معلومات التسـجيل التابعة لتثبيت التطبيقات البرمجية.

٢. سجل الأحداث المنقولة، وهو ما سنناقشه في القسم القادم.

مثال على أدلة التحليل الجنائي في نظام ويندوز:

نســتعرض هنا مثالاً مــن الحياة الواقعية على اســتخدام «عارض الأحــداث» (Event Viewer) وذلك في جمع المعلومات بهدف التحليل. ففي بعض الأحيان فإن الأحداث التي توصف بأنهــا «معلوماتية» يمكن أن تحتوي على معلومات هامة للمحلل الأمني. ويوضح الشكل (١٢-٥) لقطة من «عارض الأحداث» لجهاز مخترق.

الشكل (١٢-٥): أحداث معلوماتية

Information	5/20/2009 3:44:06 AM	SceCli	1704	None
Information	5/19/2009 10:27:07 PM	AdsmClientService	4100	None
Information	5/19/2009 2:51:56 PM	McLogEvent	5000	None
Information	5/19/2009 2:27:06 PM	AdsmClientService	4100	None
Information	5/19/2009 2:27:02 PM	AdsmClientService	4097	None
Information	5/19/2009 2:27:02 PM	AdsmClientService	4101	None
Information	5/19/2009 2:27:02 PM	AdsmClientService	4097	None
Information	5/19/2009 2:27:02 PM	AdsmClientService	4097	None
Information	5/19/2009 2:27:02 PM	AdsmClientService	4097	None

Event 5000, McLogEvent

General | Details

The description for Event ID 5000 from source McLogEvent cannot be found. Either the component that raises this event is not installed on your local computer or the installation is corrupted. You can install or repair the component on the local computer.

If the event originated on another computer, the display information had to be saved with the event.

The following information was included with the event:

524906
None
None
None
VirusScan Enterprise
5.3.00
5620

وكما تلاحــظ أن تثبيت برنامج مكافحة الفيروســات (McAfee) يعمل في هذا الجهاز. ومــن خلال تصفح ملف الســجل نلاحــظ أن بعض الكلمات تظهر على الفور. وفي قســم الوصف العام نرى «مُعرِف الحدث ٥٠٠٠» (Event ID 5000). وهذا ليس الجهاز الأصلي الذي تم تصدير السجل منه لذلك لا يمكن لنظام التشغيل ويندوز معرفة الحالة التي أدت إلى هــذا الحدث. لكن المعلومات المُدرجة تشــير إلى تطبيــق (VirusScan Enterprise) بأنــه المتهــم بالجريمة. وإذا كنت على عِلم بالمنظمة فســتعرف أن إصدار برنامج مكافحة الفيروســات في وقت الحادث هو (٥,٤,١) (مقارنة بالإصدار (٥,٣,٠) الموجود في الســجل)، كــما أن إصدار توقيعات الفيروســات هو ٥٧٠٠، مما يدل على أن ماســح الفيروســات غير مُحــدث في هــذا الجهــاز. وعند البحث في الإنترنــت عــن (Event ID 5000) وعلاقته بـ (McAfee) نكتشــف أن ذلك قد يكون الخطأ بســبب عدم التشغيل الناجح لخدمة (On Access protection) وهي الخدمة التي تحمي الجهاز من الإصابة في الوقت الفعلي.

كل هذه المعلومات حصلنا عليها من سجل بسيط للحدث المعلوماتي. وينبغي أن تتساءل في هذه المرحلة: هل كان التطبيق البرمجي لمكافحة الفيروسات يعمل في هذا الجهاز؟

أهمية الحدث:

رسائل السجل يتم تمييزها أيضاً بإشارات تدل على درجة أهميتها. فعند القاء نظرة على برنامج «عارض الأحداث» سـنلاحظ أن مجلـد العرض المخصص (Custom View) يحتوي على العرض المخصص الخاص بـ «الأحـداث الإدارية» (Administrative Events). وهذا العرض يأتي مثبتاً بشـكل افتراضي مع ويندوز ٨ ويقدم ملخصاً لجميع الأحداث «الحرجة» و«الخاطئة» و«التحذيرية» من بين جميع السـجلات الإدارية. وتُعد رسـائل السجل هذه ذات مسـتوى عـالي وذات أهمية قصـوى في نظام ويندوز. ويوضح الشـكل (١٢-٦) أحد المُخرجـات التقليدية لعرض «الأحداث الإدارية». ووفقاً لمايكروسـوفت[1] فإن مسـتويات الأهمية في ويندوز تتمثل فيما يلي:

- **المعلومـات:** الحدث الذي يصـف العملية الناجحة لمهمة مثـل تطبيق، أو برنامج تشـغيل، أو خدمة. على سبيل المثال، يتم تسـجيل الحدث المعلوماتي عند تحميل برنامج تشغيل الشبكة بنجاح.

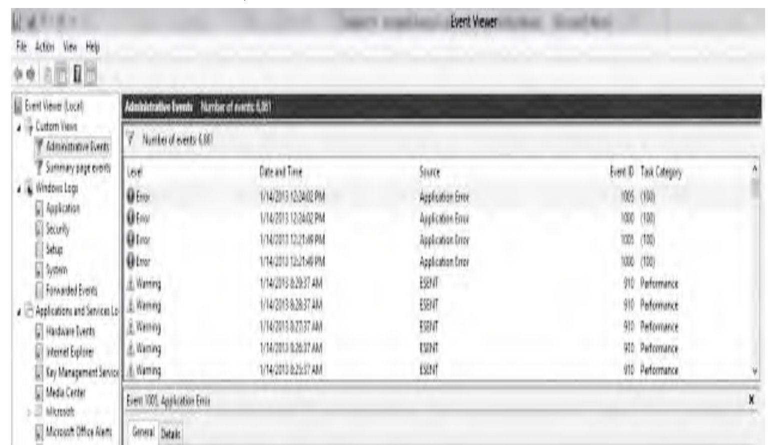
- **الإنـذار:** الحدث الذي لا يكون مهماً بالضرورة، لكنه قد يشـير إلى إمكانية حدوث مشكلة في المستقبل. على سبيل المثال، يتم تسجيل حدث إنذار عندما تبدأ مساحة القرص بالانخفاض.

- **الخطأ:** الحدث الذي يصف مشـكلة كبيرة مثل فشـل إحدى المهام الحرجة. وهذا الحدث قد يشمل فقدان بيانات أو فقدان الوظيفة. على سبيل المثال، يتم تسجيل (حدث خطأ) عند فشل تحميل الخدمة وذلك عند بدء التشغيل.

- **تدقيق النجاح (سـجل أمني):** الحدث الذي يصف الانتهاء بنجاح من حدث أمني تمت مراجعته. على سـبيل المثال، يتم تسـجيل (حدث تدقيق النجاح) عندما يقوم المستخدم بتسجيل الدخول إلى جهاز الحاسب الآلي.

(1) «How to view and manage Event Logs,» http://support.microsoft.com/kb/308427

الشكل (١٢-٦): نافذة عرض «الأحداث الإدارية»



- **تدقيق الفشل (سجل أمني):** الحدث الذي يصف الانتهاء بفشل حدث أمني تمت مراجعته. على سبيل المثال، يتم تسجيل حدث تدقيق الفشل عند عدم تمكن المستخدم من الوصول إلى برنامج تشغيل الشبكة.

ويحتوي نظام ينكس أيضاً على مستويات أهمية مشابهة لكنها تختلف بعض الشيء. وسوف نستخدم المستويات الأهمية في نظام ينكس في القسم التالي.

وعند اختيار الجانب الأيسر من «عارض الأحداث (المحلي)»، ينتقل المسؤول إلى صفحة الموجز واللمحة العامة (Overview and Summary page).

سجلات نظام ينكس:

سنُلقي الآن نظرة على سجل نظام ينكس. وفي الأقسام القادمة سنستخدم (لينكس) لكن الفكرة نفسه تنطبق أيضاً على الأنواع الأخرى من نظام ينكس مثل (Solaris) و(AIX)، وتنطبق في كثير من الأحيان على مواقع الملفات وملفات التهيئة. على سبيل المثال، أحد الملفات التي سنتعامل معها هو ملف (/var/adm/messages) في نظام (Solaris) أو ملف (var/log/messages) في نظام (Linux). وهما الملف نفسه وبالمحتويات نفسها لكن في أماكن مختلفة قليلاً.

أداة سجل النظام (Syslog):

يتضمن نظام ينكس عملية مصممة خصيصاً لتعامل الرسائل مع البرمجيات التي يمكنها التواصل مع أداة سجل النظام (syslog). وبذلك يتمكن أي مُبرمج من استخدام الأداة لحفظ معلومات السجل في مكان محدد من ملف التهيئة (syslog.conf).

ويتم استخدام أداة (syslog) من خلال تعيين ما يُعرف بالمحددات. وتتكون المُحددات من جُزئين:

1. الأداة وتحدد الخدمة المسؤولة عن انشاء رسالة الخطأ. وبعض الأدوات المتاحة هي (lpr)، (kern)، (daemon)، (cron)، (authpriv)، (auth)، و(mail). ويتم تسجيل رسائل السجل الناتجة عن نظام البريد الإلكتروني، على سبيل المثال، باستخدام أداة (mail). وتوفر (syslog) بعض الأدوات لاستخدامها في الرموز البرمجية المطورة داخلياً. وتُعرف هذه الأدوات بـ (local0)، و(local1)، وحتى (local7).
2. الأولوية وهي عبارة عمّا يلي: (debug)، (info)، (notice)، (warning)، (warn) (نفس warning)، (err)، (error نفس err)، (crit)، (alert)، (emerg)، و(panic) (نفس emerg). والأولوية تُصنف الرسالة اعتماداً على الأهمية. وتُعد الأولوية مضافة مما يعني أنه عندما يتم إرسال محدد الأولوية فإنه سيتم تسجيل جميع الأولويات الأعلى. مثلاً، المحدد (mail.warn) يتطابق مع الرسائل التي تحمل الأولوية (crit)، (err)، (warn)، و(emerg).

ويتكون ملف التهيئة من خلال دمج المُحدد مع الإجراء. والإجراء المحتمل يمكن أن يكون:

- اسم ملف مثل (var/adm/messages).
- تمرير إلى خدمة (syslog) في مضيف آخر مثل (hostname@).
- كتابة معلومات السجل إلى شاشة المستخدم من خلال تحديد اسم المستخدم أو جميع المستخدمين.

وهنا بعض الأمثلة:

```
*.info;mail.none;authpriv.none;cron.none    /var/log/messages
authpriv.*
/var/log/secure
mail.*
/var/log/maillog
cron.*                              /var/log/cron
*.emerg                              *
```

في السـطر الأول تم تصنيف جميع الرسائل على أنها رسائل معلوماتية أو تصنيف أعلى أهمية من ذلك بغض النظر عن الأداة المستخدمة. لذا سيتم كتابة (*.info) في ملف (/var/log/messages). والاسـتثناء الوحيد لهذه القاعدة هي الرسـائل التي تحتوي على أدوات البريد مثل (mail)، و(authpriv)، و(cron). وفي السـطور ٢-٤ سيتم كتابة جميع الرسائل التي تحتوي على هذه الأدوات في ملف السجل الخاص بها. وأخيراً فإن جميع الرسائل ذات الأهمية (emerg) (والتي تسـتخدم عادة في حالة إغلاق النظام) يتم عرضها على شاشـات المستخدمين الذين قاموا بتسجيل الدخول إلى الخادم.

هنـاك الكثيـر من المعلومات حول تهيئة سـجل النظام (syslog). كمـا أن هناك العديد من البدائـل لسـجل النظام، منهـا ما هو مفتوح المصـدر، ومنها ما هو تجـاري، وذلك مع وجود تحسـينات مثل تسـجيل الدخول إلى قاعدة البيانات. وللأسـف فإن هذه الموضوعات خارج نطاق هذا الكتاب. والهدف من التعرض لهذا الموضوع، سواء في نظام ويندوز أو نظام ينكس، هو توفير الخلفية اللازمة لفهم البحث عن السـجلات. وإذا كنت مشـاركاً في عملية التحقيق ونظرت في دليل (/var/log) وكانت جميع الملفات فارغة فإن ذلك لا يدل على أن شـخصاً ما قام بإزالتها. بل قد يرجع ذلك لأن المسؤول وضع السجلات في مكان آخر.

ملفات السجل الموحدة:

عند التحقيق في حادث أمني فإن المُحلل سـينظر في جميع ملفات الدليل التالي (/var/log). وفيما يلي نستعرض بعضاً من أهم تلك الملفات.

الرســائل أو ســجل النظام (syslog) وتحتوي معظم تطبيقات ينكس على ملف رسائل، لكــن بعض إصدارات ينكس تســتخدم الملــف التــالي (/var/log/syslog) بدلاً عن ملف الرسائل. ومع ذلك فإن المعلومات التي تخزنها تلك الملفات هي المعلومات نفسها الموجودة في ملف (/var/log/messages). وتذهب جميع الرسائل المعلوماتية التي تستخدم خدمة (syslog) إلى هــذه الملفات. ولذلك فإن هذه الملفات هي المحطة الأولى للمســؤول الذي يبحــث عن المشــكلات المحتملة، أو المحطــة الأولى للمحلل الأمني الــذي يبحث عن آثار الاختراق.

ومن الجدير بالذكر أنه يمكن القيام بالفحص الدقيق لملفات سجل نظام ينكس باستخدام الأدوات التي تعرضنا لها لحد الآن. خذ على ســبيل المثال الشــكل (١٢-٧) حيث تم تفريغ هذا الجزء من ملف السجل إلى الشاشة باستخدام الأمر التالي:

```
zcat syslog.?.gz| grep –v snort | grep –v AptDaemon | grep –v dbus | less
```

الشكل (١٢-٧): دليل من ملف سجل النظام (syslog)

```
Jan 13 07:30:01 inigo CRON[30617]: (root) CMD (start -q anacron || :)
Jan 13 07:30:01 inigo anacron[30620]: Anacron 2.3 started on 2013-01-13
Jan 13 07:30:01 inigo anacron[30620]: Will run job `cron.daily' in 5 min.
Jan 13 07:30:01 inigo anacron[30620]: Jobs will be executed sequentially
Jan 13 07:35:01 inigo anacron[30620]: Job `cron.daily' started
Jan 13 07:35:01 inigo anacron[30687]: Updated timestamp for job `cron.daily' to 2013-01-13
Jan 13 07:56:58 inigo cracklib: no dictionary update necessary.
Jan 13 07:57:09 inigo rsyslogd: [origin software="rsyslogd" swVersion="5.8.6" x-pid="722" x-info="http://www.rsyslog.com"] rsyslogd was HUPed
Jan 11 07:38:16 inigo kernel: [337129.385557] device eth0 left promiscuous mode
Jan 11 07:38:17 inigo rsyslogd-2177: imuxsock begins to drop messages from pid 5380 due to rate-limiting
Jan 11 07:38:17 inigo rsyslogd-2177: imuxsock begins to drop messages from pid 24379 due to rate-limiting
Jan 11 07:38:19 inigo kernel: [337131.708016] device eth0 entered promiscuous mode
Jan 11 07:38:25 inigo anacron[24018]: Job `cron.daily' terminated (exit status: 1) (mailing output)
Jan 11 07:38:25 inigo anacron[24018]: Can't find sendmail at /usr/sbin/sendmail, not mailing output
Jan 11 07:38:25 inigo anacron[24018]: Normal exit (1 job run)
Jan 11 08:17:01 inigo CRON[24910]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Jan 11 09:17:01 inigo CRON[25618]: (root) CMD (   cd / && run-parts --report /etc/cron.hourly)
Jan 11 09:17:49 inigo dhclient: DHCPREQUEST of 131.247.96.1 on eth0 to 131.247.174.245 port 67
```

وهذا الأمر يوجه النظام بفك الضغط عن جميع محتويات الملفات في الدليل الحالي بدءاً من مطابقة النمط أعلاه حيث تتســع علامة الاســتفهام (?) لأي حرف أو رقم. وبعد ذلك يقوم الأمر بإزالة أي ســطر يحتوي على (snort)، أو (AptDaemon)، أو (dbus) ومن ثم

يقوم بعرض النتائج من خلال أمر الاستدعاء (less). والهدف من القيام بذلك هو تنظيف ملف السجل. وفي سجل أحداث نظام ويندوز، سيكون ذلك مشابهاً للطلب من البرنامج بإخفاء رسائل «تدقيق النجاح» (Success Audit) للمبتدئين. وهذا الأمر البسيط يُخفِض عدد الأسطر من ٣٦٠٠ سطر إلى ١٠٠٠ سطر فقط.

والسبب وراء عملية التنظيف هذه واضح. فعندما تبدأ بفحص ملفات السجل فإنك تريد أن تنظر في الأحداث الشاذة والغريبة. انظر في الشكل (١٢-٧) مرة أخرى. في منتصف الشكل تقريباً يظهر لك سطر السجل التالي:

```
Jan 11 07:38:16 inigo kernel: [337129.385557] device eth0 left promiscuous mode
```

جميع سطور السجل التي تستخدم خدمة (syslog) تتبع النمط نفسه: أولاً التاريخ، ثم الوقت، واسم المضيف، وخدمة تسجيل الرسالة، وأخيراً الرسالة الفعلية. وهذا السطر بالتحديد يُبين أنه في الساعة (٧:٣٨) وفي يوم (Jan 11) أصبح وضع واجهة (eth0)، وهي الواجهة السلكية التي تربط المضيف بالشبكة، غير جيد «left promiscuous mode». وهذا عادة يمثل مصدراً للقلق لأن الواجهة التي تكون في هذا الوضع تصبح قادرة على التقاط جميع البيانات التي تراها بما في ذلك حزم البيانات التي لا تنتمي لها. وفي بيئة منفصلة قد لا يُمثل ذلك مشكلة. لكن في بيئة مشتركة، مثل نقاط الوصول غير المحمية، فإن حركة المرور من جميع الأجهزة المتصلة بنقطة الوصول ستكون واضحة لجهاز الحاسب الآلي في وضع (promiscuous mode).

سجل المصادقة:

وينبغي أن يكون سجل المصادقة هو محطة التوقف الثانية لمُحلل الأمن. وهذا السجل موجود في ملف (/var/log/secure) أو ملف (/var/log/auth.log) حسب اختلاف نظام التشغيل. وكما يدل الاسم فإن هذا الملف يحتوي على معلومات المصادقة ومعلومات التخويل على النظام. ويوضح الشكل (١٢-٨) هذا الملف.

الشكل (١٢-٨): ملف (auth.log)

```
Jan 14 00:17:01 inigo CRON[10982]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 00:17:01 inigo CRON[10982]: pam_unix(cron:session): session closed for user root
Jan 14 00:26:15 inigo sshd[11094]: Invalid user aadriano from 66.135.32.170
Jan 14 00:26:15 inigo sshd[11094]: input_userauth_request: invalid user aadriano [preauth]
Jan 14 00:26:15 inigo sshd[11094]: pam_unix(sshd:auth): check pass; user unknown
Jan 14 00:26:15 inigo sshd[11094]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=host.insourceguy.com
Jan 14 00:26:17 inigo sshd[11094]: Failed password for invalid user aadriano from 66.135.32.170 port 47379 ssh2
Jan 14 00:26:17 inigo sshd[11094]: Received disconnect from 66.135.32.170: 11: Bye Bye [preauth]
Jan 14 01:17:01 inigo CRON[11694]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 01:17:01 inigo CRON[11694]: pam_unix(cron:session): session closed for user root
Jan 14 02:17:01 inigo CRON[12421]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 02:17:01 inigo CRON[12421]: pam_unix(cron:session): session closed for user root
Jan 14 03:17:01 inigo CRON[13133]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 03:17:01 inigo CRON[13133]: pam_unix(cron:session): session closed for user root
Jan 14 04:17:01 inigo CRON[13843]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 04:17:01 inigo CRON[13843]: pam_unix(cron:session): session closed for user root
Jan 14 05:17:01 inigo CRON[14551]: pam_unix(cron:session): session opened for user root by (uid=0)
Jan 14 05:17:01 inigo CRON[14551]: pam_unix(cron:session): session closed for user root
Jan 14 05:35:10 inigo sshd[14767]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=5.79.16.183  user=root
Jan 14 05:35:12 inigo sshd[14767]: Failed password for root from 5.79.16.183 port 42917 ssh2
Jan 14 05:35:12 inigo sshd[14767]: Received disconnect from 5.79.16.183: 11: Bye Bye [preauth]
Jan 14 05:35:18 inigo sshd[14769]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=5.79.16.183  user=root
Jan 14 05:35:19 inigo sshd[14769]: Failed password for root from 5.79.16.183 port 43352 ssh2
Jan 14 05:35:19 inigo sshd[14769]: Received disconnect from 5.79.16.183: 11: Bye Bye [preauth]
Jan 14 05:35:25 inigo sshd[14773]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=5.79.16.183  user=root
Jan 14 05:35:27 inigo sshd[14773]: Failed password for root from 5.79.16.183 port 43658 ssh2
Jan 14 05:35:27 inigo sshd[14773]: Received disconnect from 5.79.16.183: 11: Bye Bye [preauth]
Jan 14 05:35:33 inigo sshd[14777]: pam_unix(sshd:auth): authentication failure; logname= uid=0 euid=0 tty=ssh ruser= rhost=5.79.16.183  user=root
Jan 14 05:35:35 inigo sshd[14777]: Failed password for root from 5.79.16.183 port 43746 ssh2
Jan 14 05:35:35 inigo sshd[14777]: Received disconnect from 5.79.16.183: 11: Bye Bye [preauth]
Jan 14 06:17:01 inigo CRON[15272]: pam_unix(cron:session): session opened for user root by (uid=0)
```

وتم استخراج هذا الملف من صندوق لينكس المكتبي والذي لا يحتوي على أي بيانات جاذبة لقراصنة الحاسب. ويُعرف هذا الصندوق بمحطة «التحطم والاحتراق» (crash and burn). ويتم إعداد هذا الصندوق ثم تدميره ثم إعداده مرة أخرى وهكذا. والهدف منه هو اختبار أدوات التحليل الجنائي الجديدة.

وبالنظر مرة أخرى إلى ملف السجل، تبين أنه في الليلة السابقة حدث ما يلي خلال ٦ ساعات:

- شخص ما يحاول تسجيل الدخول باسم (aadriano) وذلك باستخدام (ssh) من (٦٦,١٣٥,٣٢,١٧٠).
- شخص ما يحاول تسجيل الدخول مرات متتالية، وباستخدام العديد من كلمات المرور، إلى حساب الجذر من (٥,٧٦,١٦,١٨٣)

ولأنه لا يوجد هناك مُستخدم باسم (aadriano) في هذا الصندوق، لا يمكننا إلا الافتراض بأن هذا نص برمجي آلي ربما يستخدم كلمة مرور معروفة تم الحصول عليها من مكان ما للمستخدم (aadriano). وعند القيام ببحث سريع على الشبكة للحساب ولعنوان بروتوكول الإنترنت، تم الحصول على صفحة من موقع (honeypot) وهو موقع مفتوح عمداً، وذلك لجذب وتسجيل محاولات التسلل. ويحتوي موقع (honeypot) على كلمات المرور الفعلية المُستخدمة ضده للحسابات (aadriano)، (aadriano123)، (admin). وجميع المحاولات المسجلة في موقع (honeypot) حدثت في التاريخ نفسه الذي وقعت فيه الحادثة الخاصة بهذا المثال.

وفي الواقــع فــإن النقطة التالية مثيرة للقلق، وهي أن عنــوان بروتوكول الإنترنت يخص شركة اتصالات في روســيا. وعند القيام بالبحث على الإنترنت، لم نتوصل لأي ســجلات ولأي أثر في أي مكان. وفي حين يوجد دليل واضح على أن الهجمة الأولى كانت هجمة آلية، فإن الهجمة الثانية ربما كانت هجمة استكشــافية. إذاً تكون الخطوة التالية في عملية التحليل على النحو التالي:

التحقق من إصابة أجهزة أخرى في المنظمة بنفس عنوان بروتوكول الإنترنت.

فحص السجل كاملاً، دون تصفية، وذلك لنفس عنوان بروتوكول الإنترنت.

فحص ملفات السجل الأخرى في نفس الجهاز.

إجراءات العمل الموحدة لقراصنة الحاسب

بمجــرد أن تعتــاد على تحليل الحوادث ســتلاحظ وجــود نمط. قراصنة الحاســب المجرمون والمنظمــون والذين يقومون بهجمات جماعية عادة يقســمون أنشــطتهم إلــى ثلاث مراحل مختلفة لثلاث فِرق مختلفة تعمل في ثلاث مناطق مختلفة:

تأتي أولاً مرحلة **الاكتشــاف** والتي تتمثل في اللمســات الناعمة على البنيــة التحتية من أجل اكتشاف وتحليل نقاط الضعف المحتملة. مسح المنافذ، ومحاولات تسجيل الدخول المحدودة كما رأينا في هذا القســم، ومســح خادم الشــبكة بحثاً عن التطبيقات الضعيفة، كل ذلك أمثلة للبحث عن نقاط الضعف المحتملة في مرحلة الاستكشاف.

وبعد مرحلة الاكتشــاف تبــدأ مرحلة **الاختــراق**. والهدف من مرحلة الاختراق هو اســتخدام المعلومات المُكتشــفة في المرحلة الأولى لوضع موطئ قدم في المنظمة المستهدفة. ويقوم فريق مرحلة الاكتشــاف بتســليم المعلومات لفريق مرحلة الاختراق، وذلــك للقيام بالاختراق الفعلــي. وحتى لــو كانت النُظم الموجودة فــي المنظمة ذكية بما فيــه الكفاية للقيام بمنع التواصل مع المجموعة الأولى من عناوين بروتوكول الإنترنت المشــمولة في مرحلة الاكتشاف، فإن المرحلة الثانية تســتخدم عناوين جديدة كمصدر للهجوم. ومن ثم فلن يتم حظر نشــاط مرحلة الاختراق.

وأخيراً تأتي مرحلة **الاستغلال**. وفي هذه المرحلة قد يتم استخراج بعض البيانات من الأجهزة المخترقة. وقد تُســتخدم بعض الأجهزة لاســتغلال منظمات أخرى. وبعــض الأجهزة قد تُترك خاملة أملاً في عدم اكتشافها والتوسع في عملية الاستغلال.

ملــف (wtmp): وهو ليس ملــف نصي بل هو ملف ثنائي يحفظ معلومات تســجيل الدخــول والخروج الســابقة. والأمــر (who) في نظام ينكس يقوم بقــراءة ملف (/var//log/wtmp) ويعرض على الشاشــة قائمة بآخر المســتخدمين الذين قاموا بتسجيل الدخول. وبالإضافة إلى ذلك فإن الأمر (last) يقوم بتســجيل محاولات إعادة تشغيل النظام في ملف (/var/log/wtmp/). وإذا كنــت تبحــث عــن عدد مرات إعادة تشــغيل النظام فإن الأمر (last) هو أسهل الأوامر للتشغيل والحصول على النتيجة. والافتراض هنا بطبيعة الحال أن الســجل الأخير لم يتم تغييره. ويوضح الشــكل (١٢-٩) مثالاً على مخرجات الأمر (last) في أحد أجهزة لينكس المكتبية. ويحتوي الشــكل على اسم المستخدم، ورقم المحطة المستعارة المرتبطة بتســجيل الدخول، واســم المضيف، والفترة الزمنية التي قام المســتخدم بتسجيل الدخول فيها. أما مفتاح (a-) في نهاية الأمر فهو يطلب من النظام عرض اســم المضيف في نهاية السطر. وإذا لم يتم استخدام هذا المفتاح، فإن عرض اسم المضيف سيكون في العمود الثالث ويُقتطع منه حسب الحاجة، مما يجعل قراءة اسم المضيف كاملاً أمراً صعباً.

الشكل (١٢-٩): مثال على مخرجات الأمر (last)

```
[2020][campoe.inigo: /var/log]$ last -a
campoe   pts/5        Tue Jan 22 09:13   still logged in    spinoza.acomp.usf.edu
campoe   pts/5        Thu Jan 17 21:55 - 00:31  (02:35)     pool-71-251-115-226.tampfl.fios.verizon.
net
campoe   pts/2        Mon Jan 14 10:25   still logged in    :0
campoe   tty7         Mon Jan  7 10:01   still logged in    :0
(unknown tty7         Mon Jan  7 10:00 - 10:01  (00:01)     :0
reboot   system boot  Mon Jan  7 10:00 - 09:25 (14+23:24)   3.5.0-22-generic

wtmp begins Mon Jan  7 09:54:17 2013
[2021][campoe.inigo: /var/log]$ ■
```

ويتم تدوير ملف (wtmp) بشــكل دوري. وتجــدر ملاحظة وجود العديد من ملفات (wtmp) في (/var/log/) والمنتهية بـ ١، ٢، وهكذا. ويمكن الوصول إلى هذه الملفات القديمة باستخدام الأمر (last) مع (a-f <filename>).

الصديق المفضل لمسؤول النظام

بإمكانك معرفة الكثير عن أوامر ينكس وعن جميع المفاتيح والخيارات المتاحة باستخدام الأمر (man). على سبيل المثال، الأمر (man last) سيعطيك وصفاً كاملاً للأمر، كما يعطيك مؤشر على مكان وجود ملف السجل في النظام. كما أن صفحات الأمر (man) توضح الأوامر ذات الصلة التي قد تكون مفيدة.

ملف (utmp): في حين أن ملف (wtmp) يحفظ معلومات تسـجيل الدخول والخروج السابقة، فإن ملف (utmp) يشير إلى مَن قام بتسجيل الدخول في الوقت الراهن. وفي بعض أنظمة ينكس، يتم الاحتفاظ بملف (utmp) في دليل (/var/adm/). لكن معظم توزيعات نظام ينكس تحتفظ بالملف في دليل (/var/run/).

وبشـكل مشـابه لملف (wtmp)، فإن ملـف (utmp) ملف ثنائي أيضـاً. ويتم فحص محتويات هذا الملف باسـتخدام الأمـر (who). ويقوم هذا الأمر بقـراءة ملف (utmp) ومن ثم عرض اسم المستخدم الذي قام بتسجيل الدخول، كما يقوم هذا الأمر بعرض بعض المعلومات عن مكان تسجيل الدخول.

أمر مفيد آخر هو الأمر (w) والموضح في الشكل (١٢-١٠). ويعرض هذا الأمر معلومات عـن النظام، كما يعـد هذا الأمر من أول الأوامر التي يقوم محلل النظام بتشـغيلها عندما يقوم بتسجيل الدخول. ويقوم الأمر (w) بعرض ما يلي:

- منذ متى يعمل جهاز الحاسب الآلي بدءاً من آخر إعادة تشغيل.
- ما المحطات الحقيقة أو المستعارة المستخدمة.
- متى قام المستخدم بتسجيل الدخول.
- هل المستخدم نشط أم لا؟
- معلومات الحِمل.
- الأوامر التي تعمل بواسطة المستخدم.

الشكل (١٢-١٠): مخرجات الأمر (w)

```
[2033][campoe.inigo: /var/log]$ w
 09:53:28 up 14 days, 23:54,  3 users,  load average: 0.13, 0.08, 0.06
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU WHAT
campoe   tty7     :0                07Jan13 14days  4:22m  0.05s gdm-session-worker [pam/gdm-passwor
campoe   pts/2    :0                14Jan13 42:05   0.21s  0.21s bash
campoe   pts/5    spinoza.acomp.us 09:13    0.00s  0.12s  0.00s w
[2034][campoe.inigo: /var/log]$ ■
```

قد لا تكون مخرجات الأمر (w) الموضحة في الشكل (١٢-١٠) مؤثرة جداً، لكنها تصبح مفيدة جداً في الأنظمة ذات المستخدمين المتعددين حيث يقوم مئات المستخدمين بتسجيل الدخول في نفس الوقت. دعنا نفترض أنه أثناء تنفيذ الأمر (w) لاحظت أن أحد المستخدمين يشغل الأمر التالي:

```
nmap 192.168.1.024/ > ~/.out/.output.pscan
```

وحتى إذا كنت لا تعلم ما يقوم به الأمر (nmap)، فإن حقيقة وجود مستخدم للنظام يقوم بحفظ بيانات في ملف مخفي وفي دليل مخفي يجب أن يقرع أجراس التحذير. وعند البحث على الإنترنت عن الأمر (nmap) نجد أنه ماسح قوي للمنافذ. وتشير مواصفات المُضيف إلى أن هذا المستخدم يقوم بمسح كامل للشبكة الفرعية (١٩٢,١٦٨,١). وحتى لو لم يكن ذلك مخالفاً لسياسة المنظمة، فإنه يستحق الفحص والتدقيق. وإذا كان عمود (FROM) يعرض لك اسم مضيف ليس معروفاً لك، فإنه قد يكون حان الوقت للدخول في وضع الاستجابة للحوادث.

سجل خادم الشبكة:

معظم الحوادث الأمنية التي حدثت في السنوات القليلة الماضية كانت تستهدف أحداثاً على شبكة الإنترنت سواء كانت استغلال ثغرات جافا، أو تحميل ملف بي دي اف (PDF) مُلوث، أو هجمات حقن تعليمات الاستعلام البُنيوية (SQL injection) الشائعة. ولتحليل هذه الأحداث نحتاج إلى عينة من سجل خادم الشبكة.

والمربع التالي يوضح بعض الأسطر لملف سجل خادم تطبيقات. وهذا الخادم يشغل تطبيق (PeopleSoft)، والذي يستخدم بدوره خادم مخصص يسمى خادم ويب أباتشي (Apache web server)، حيث يستخدم التطبيق هذا الخادم في واجهته الأمامية.

```
xxx.2xx.89.16 - -  [09/May/2012:11:41:37 -0400] «GET /login HTTP/1.1»
404 338
xxx.2xx.89.16 - -   [09/May/2012:11:41:37 -0400] «GET /sws/data/sws_
data.js HTTP/1.1»  404 353
xxx.2xx.89.16 - -  [09/May/2012:11:41:37 -0400] «GET /wcd/system.xml
HTTP/1.1» 404 347
xxx.2xx.89.16 - -   [09/May/2012:11:41:37 -0400] «GET /js/Device.js
HTTP/1.1» 404 345
xxx.2xx.89.16 - - [09/May/2012:11:41:37 -0400] «GET /ptz.htm HTTP/1.1»
404 340
xxx.2xx.97.183 - -  [09/May/2012:11:41:37 -0400] «GET / HTTP/1.1» 200
14257
xxx.2xx.97.183 - -  [09/May/2012:11:41:37 -0400] «GET /authenticate/
login HTTP/1.1» 404 352
xxx.2xx.97.183 - - [09/May/2012:11:41:37 -0400] «GET /tmui/ HTTP/1.1»
404 339
xxx.2xx.97.183 - -  [09/May/2012:11:41:37 -0400] «GET /admin/login.do
HTTP/1.1» 404 348
xxx.2xx.97.183 - -  [09/May/2012:11:41:37 -0400] «GET /dms2/Login.jsp
HTTP/1.1» 404 348
xxx.2xx.97.183 - - [09/May/2012:11:41:37 -0400] «GET /login HTTP/1.1»
404 339
xxx.2xx.97.183 - - [09/May/2012:11:41:38 -0400] «GET /sws/data/sws_
data.js HTTP/1.1» 404 354
xxx.2xx.97.183 - - [09/May/2012:11:41:38 -0400] «GET /wcd/system.xml
HTTP/1.1» 404 348
xxx.2xx.97.183 - -  [09/May/2012:11:41:38 -0400] «GET /js/Device.js
HTTP/1.1» 404 346
xxx.2xx.97.183 - -     [09/May/2012:11:41:38 -0400] «GET /ptz.htm
HTTP/1.1» 404 341
xxx.2xx.89.16 - -   [09/May/2012:11:41:38 -0400] «GET /robots.txt
HTTP/1.1» 404 343
xxx.2xx.89.16 - -  [09/May/2012:11:41:38 -0400] «GET /CVS/Entries
HTTP/1.1» 404 344
xxx.2xx.89.16 - -        [09/May/2012:11:41:38 -0400]   «GET   /
NonExistant1380414953/ HTTP/1.1» 404 355
```

في العينة أعلاه يبدو أن المُضيف (٩٧,١٨٣) يقوم بنوع من البحث على خادم الشـبكة. ويبدو أن كل سـطر يبحث عن تطبيق مختلف. مرة أخرى وباسـتخدام البحث على شبكة الإنترنـت اتضح أن (ptz.htm) هي الواجهـة الأمامية للكاميرا الأمنية (AXIS). كما اتضح أن ملـف (sws_data.js) ينتمي إلى حزمة (Awstats) وهي حزمة إحصاءات على شـبكة الإنترنت. وبالإضافة إلى هذه النتائج، يبدو أن المُضيف (٩٧,١٨٣) يهاجم المُضيف (٨٩,١٦) والـذي يقوم بدوره بتمرير الهجوم إلى خادم الشـبكة. وفي الواقـع، بعد القيام بمزيد من التحقيق اتضح أن مُضيف (٨٩,١٦) هو خادم وكيل لتطبيق (Peoplesoft).

سجل بروتوكول (Netflow):

بروتوكـول (Netflow) هـو بروتوكول شـبكي طُـور من قبل شركة سيسـكو (Cisco) بهدف جمع معلومات حركة مرور الشبكة المتعلقة ببروتوكول الإنترنت (IP). وأصبح هذا البروتوكول خلال السـنوات الماضية معياراً لهذا النوع من السجلات حيث أصبح البروتوكول مدعوماً من قبل موردي الأجهزة الشبكية الأخرى.

وفيما يلي نعرض عينة من المعلومات المتوفرة من بروتوكول (Netflow).

```
Date      Time       Source      Port  Destination   Port
Packets
201166.2 00:11:19.285 01-12-xx.71.155 34340  1xx.2xx.222.243 443
TCP 1 60
201161.1 00:11:46.659 01-12-xx.172.2  35590  1xx.2xx.222.243  80
TCP 1 48
201171 00:18:58.992 01-12-.xx.61.163  55194  1xx.2xx.222.243  80
TCP 3 152
201166.2 00:18:59.594 01-12-xx.71.155 36614  1xx.2xx.222.243 443
TCP 3 180
```

ويُعد سـجل بروتوكـول (Netflow) مفتاح المقدرة على تكوين علاقات بين الأنشـطة في الأجهـزة المتعـددة على الشـبكة. وبالإضافـة إلى تحديد الوقت فإن سـجل بروتوكول (Netflow) قـادر على تحديد مصـدر ووجهة المعاملات. ويُعد رقم المنفذ مفيد في تحديد الخدمة قيد التشغيل على بروتوكول الإنترنت (IPs) للمصدر و/أو الوجهة. وأخيراً فإن عدد الحزم يُعد مؤشراً جيداً لكمية المعلومات التي يتم تبادلها خلال هذا التواصل. ومن المربع أعلاه يمكننا معرفة بعض الأمور:

- ربمـا يعمـل المضيف (٢٢٢,٢٤٣) على خادم ويب من خـلال منفذ رقم ٨٠. وعادة يكون رقم المنفذ هذا لخادم ويب غير آمن (non-SSL).
- يعمل نفس بروتوكول الإنترنت على خادم ويب آمن (SSL) من خلال المنفذ القياسي الخاص به رقم ٤٤٣.
- كميـة حركة المرور على هذه المنافذ تعد مؤشراً على مدى انتشـار خادم الشـبكة. وكمية التواصل غير الطبيعية قد تشير إلى علامات استفهام حول المحتوى (مثل المواد الإباحية، أو الموسيقا، أو الأفلام) الذي يُوزع بشكل غير قانوني.
- بما أنه يوجد خادم ويب قيد التشـغيل، إذاً لا بد من وجود ملف سـجل في مكان ما للمضيف (٢٢٢,٢٤٣). وإذا كنت تريد معرفة ما تم نقله في وقت محدد، تسـتطيع ذلك من خلال افتراض تزامن ساعة بروتوكول (netflow) وساعة خادم الشبكة.

وكما ترى فإنه يمكننا الحصول على قدر جيد من المعلومات من أربعة أسـطر من سجل بروتوكول (netflow).

السجلات الأخرى:

اعتماداً على التطبيقات التي تعمل في نظامك، قد يكون لديك أكثر من سـجل لفحصها أثناء العمل على تحليل الحادث. وفيما يلي بعض الرسـائل المسـتخرجة من خادم يُشـغِل تطبيـق (WordPress) وهـو أحـد أنظمـة إدارة المحتـوى (Content Management System). وتوضح هذه الرسـائل أن تطبيق (WP) تعرض لهجوم بواسطة حقن تعليمات الاستعلام البُنيوية (SQL injection).

```
[07-Dec-2012 02:40:49] WordPress database error You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version for the right syntax to use near 'WHERE id = —1\'' at line 1 for query SELECT text, author_id, date FROM WHERE id = —1\'
[07-Dec-2012 02:40:50] WordPress database error You have an error in your SQL syntax; check the manual that corresponds to your MySQL server version
for the right syntax to use near 'WHERE id = 999999.9 UNION ALL SELECT
0x31303235343830303536--' at line 1 for query SELECT text, author_id, date FROM WHERE id = 999999.9 UNION ALL SELECT 0x31303235343830303536--
```

التهيئة العامة للسجل والمحافظة عليه:

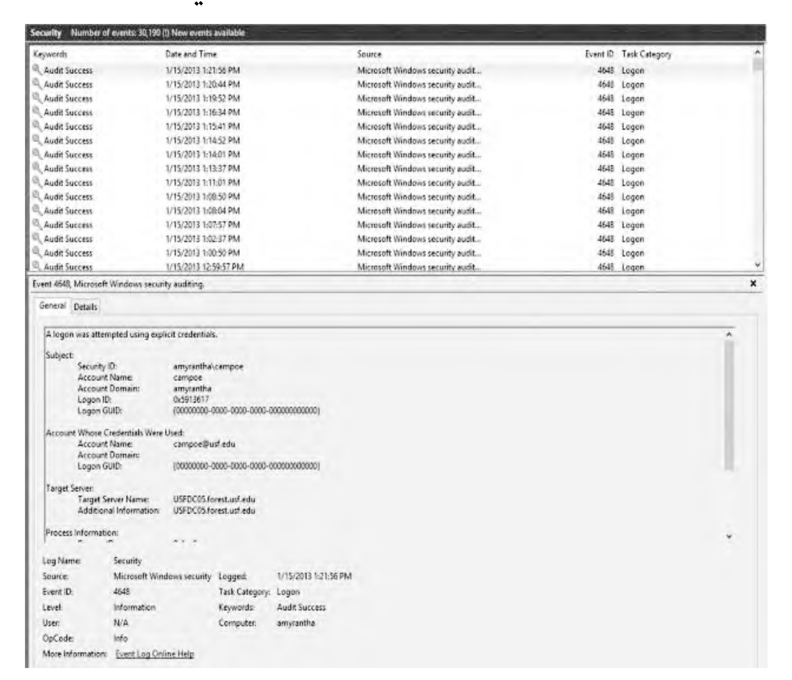
تأتي أنظمة التشغيل والتطبيقات البرمجية من المطور بإعدادات افتراضية لالتقاط السجل وهذه الإعدادات الافتراضية لا تتناسب دائماً مع النتائج المطلوبة. وكما ذكرنا في بداية هذا الكتاب، فإن موظفي تقنية المعلومات يريدون استخراج أشياء مختلفة من السجل، وما يريده المستخدم قد لا يرغب فيه المحلل الأمني. على سبيل المثال، قد لا يهتم المستخدم على الإطلاق بسجلات تسجيل الدخول وتسجيل الخروج في الأجهزة المكتبية. ومن الواضح أن هذه المعلومات قيمة جداً من وجهة نظر المحلل الأمني. لذلك فإن المهمة الأولى المطلوب إنجازها عند التعامل مع تهيئة وحفظ السجل هي تحديد الجمهور. مَن هو المهتم برؤية السجل؟ وهل هناك موضوع ذو علاقة بالامتثال ويتطلب إعداد السجل وتحديد نشاطه؟ على سبيل المثال، هل يُطلب من المنظمة من قبل مدقق الحسابات الاتحادي (Federal Auditor) أن يتم تسجيل جميع من يصل إلى أرقام الضمان الاجتماعي (Social Security Numbers) المحفوظة في قاعدة البيانات؟ هل يُطلب من المنظمة المحافظة على معلومات السجل لعدد معين من الأيام؟ وما المعلومات التي ينبغي للمنظمة المحافظة عليها؟

كل ما سبق من أسئلة لها علاقة بالامتثال، وأسئلة الامتثال ليست بالضرورة نفس الأسئلة الأمنية. الآن سنُلقي نظرة على تغييرات التهيئة الأساسية ونسأل مرة أخرى السؤال التالي: ما الذي يجب أن أحتفظ به؟ مع إبقاء أعيننا على الجانب الأمني. الشكل (١٢-١١) يوضح إدخالات سجل الأحداث الأمنية بالإعدادات الافتراضية وذلك من تثبيت الإصدار المبكر لنظام التشغيل ويندوز ٨.

ناقشنا سابقاً حقيقة أن السجل الأمني هو أسرع السجلات في الامتلاء والتدوير. والسبب في ذلك هو تسجيلات الدخول الناجحة والمتكررة من المستخدمين. وفي هذه الحالة لدينا الخيارات التالية:

- **زيادة الحد الأقصى لحجم ملف السجل:** وهذا يعطينا بعض الوقت الإضافي والذي قد يكون كافياً للسماح بعدد ملائم من الأيام للاحتفاظ بالسجل في أجهزة الحاسب الشخصية. لكن هذا الحل ليس «مناسباً للجميع» فقد لا يكون عملياً في بيئة المنظمات. فيمكن أن يقوم مسؤول النظام بتحديد أحجام سجل مختلفة لأجهزة حاسب آلي مختلفة اعتماداً على نمط الاستخدام.
- **عدم تسجيل رسائل «التدقيق الناجح»:** وقد يبدو هذا الخيار مقبولاً، على الأقل في البداية. لكن ينبغي ألا يكون الخيار الأول للمحلل الأمني. فإذا قمت بإزالة كافة التسجيلات الناجحة من السجل، فإنك لن تعرف عدد المرات التي قام قراصنة الحاسب فيها بتسجيل الدخول لجهاز الحاسب الآلي باستخدام كلمة مرور مسروقة في الساعة الرابعة صباحاً! ولمثال عملي عن ذلك انظر العمود الجانبي في الصفحة التالية.

الشكل (١٢-١١): قصاصة من السجل الأمني

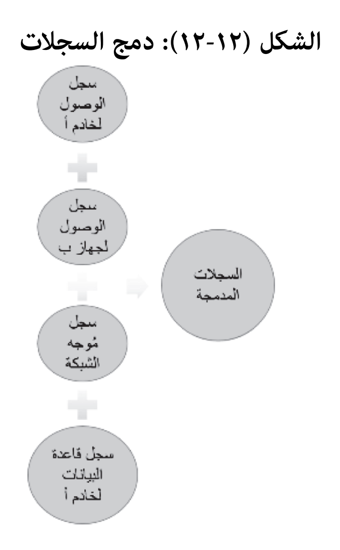


- **تدويــر وأرشــفة الملفات القديمة:** وثمــة خيار آخر يتمثل في أرشــفة الملفات وبدء ســجل جديد. وهذا الخيار جــذاب لأنه يجعل حجم ملفات الســجل صغيراً وأكثر قابلية للإدارة، كما يســاعد على الاحتفاظ بمحتويات السجل لفترة طويلة من الزمن. والنقطة الســلبية لهذا الخيار هي استخدام مساحة القرص، فلو افترضنا أنك ترغب في الاحتفاظ بالنسخ الخمس الأخيرة من ملفات السجل بحيث يكون حجم كل ملف ٢٠ ميقا بايت، فإن حجم السجل الأمني سيصل إلى ١٠٠ ميجا بايت. ماذا عن بقية ملفات السجل الأخرى؟ ولذلك فإن استخدام مساحة القرص سيكون في ازدياد.

الخيار الأفضل هو نقل ملفات السجل بعيداً إلى جهاز آخر، إذا كان ذلك ممكناً، بحيث يكــون ذلك الجهاز مخصصاً للحفاظ على معلومات الســجل. وقد تمت إضافة هذا الخيار في نظام التشــغيل ويندوز ٨. وهذه الأحداث التي يتم تصديرها ســتوضح سجل الأحداث المرسلة (Forwarded Events).

وتُعرف عملية تصدير السجل من الجهاز الأصلي إلى جهاز مركزي مخصص لتجميع السجلات بعملية دمج السجلات. ومن وجهة نظر أمنية ومن وجهة نظر الامتثال أيضاً، يعد تصدير السجلات الخيار الأفضل وذلك لعدة أسباب. بالنسبة للمبتدئين، يسمح هذا الخيار بالربط المُبسط بين السجلات وأجهزة الحاسب الآلي المختلفة. وبوجود جميع السجلات في مكان واحد، لا يحتاج المحلل الأمني للانتقال إلى عدة أماكن لجمع المعلومات. وفي الواقع فإنه من الصعب جمع السجلات خصوصاً إذا كنت لا تعرف المضيف الذي تم اختراقه. مثلاً، في حالة دمج السجلات يقوم المحلل الأمني بالنظر في ملفات الوصول بحثاً عن جميع محاولات الاتصال من بروتوكول إنترنت (IP) معين. وبذلك تكون العملية أسهل وأسرع، وهذا هو المطلوب خصوصاً عندما تكون في منتصف الحادث الأمني لأن دقائق توقف النظام قد تتحول إلى ملايين من الدولارات (الشكل ١٢-١٢).

الشكل (١٢-١٢): دمج السجلات



والخطوة الأولى التي يقوم بها قرصان الحاسب ذو الخبرة عندما يقتحم أحد أجهزة الحاسب الآلي، خصوصاً في بيئة المنظمات، هي مسح وتعطيل كل السجلات في محاولة لطمس معالم جريمته. وإذا كانت مدخلات السجلات يتم تصديرها إلى جهاز آخر فور حدوثها وفي الوقت الفعلي فإن محلل الأمن سيكون قادراً على الحصول على النسخة الأصلية من السجلات حتى في حال تلف السجلات المحلية.

ويحمي تصدير الســجلات أيضاً من خطر إســاءة استخدام الصلاحيات من قبل مسؤول النظام حيث يســتطيع مســؤول الخادم بســهولة تغطية آثاره في حال الاحتيال وذلك عن طريق تعديل معلومات الســجل. وبطبيعة الحال، هنا تنبيه: في حال إعداد جهاز مركزي لحفظ الســجلات يجب أن يتــم الوصول إليه اعتماداً على مبــدأ «الحاجة للمعرفة» فقط. والممارســة العامة هنا هي الســماح فقط لموظفي الأمن بالوصول لهــذا الجهاز، مع إعطاء صلاحية (القراءة فقط) للمسؤولين الآخرين حسب الحاجة.

الاستجابة المباشرة للحوادث الأمنية:

القاعدة الأولى للأدلة الجنائية هي اســتعادة أكبر قدر ممكن من البيانات دون تعطيل النظام إذا كان ذلك ممكناً. وفي بعض الأحيان، وتبعاً للضرر الناتج، يقوم المســؤول بسحب القابس من الجهاز أو فصل الجهاز من الشبكة، وبعد ذلك يقوم بطرح الأسئلة.

لكــن إذا كان الوضع يســمح بتحليل النظــام المخترق دون تعطيله، فــإن ذلك قد يزود المحققين بالكثير من البيانات. وتتضمن الاستجابة المباشرة للحوادث الأمنية بيانات مستقرة وبيانات غير مســتقرة. البيانات المستقرة هي البيانات المحفوظة في أجهزة حِفظ دائمة مثل الأقــراص الصلبــة. أما البيانات غير المســتقرة فهي البيانات التي تُفقد عند إعادة تشــغيل النظام مثل العمليات الجارية، ومحتوى الذاكرة المتنقلة، واتصالات بروتوكول التحكم بالنقل (TCP) وبروتوكــول وحدة البيانات المســتخدمة (UDP)، وغيرها. وعند الانتهاء من جمع تلك البيانات فإنه يتم نقلها من الجهاز من خلال أي وسيلة ممكنة. ومن التطبيقات الشائعة المستخدمة في نقل تلك البيانات إلى محطة أخرى (والتي تعرف عادة بمحطة التحليل الجنائي) تطبيــق (netcat) وتطبيق (cryptcat). ويعمل تطبيق (netcat) على إنشــاء قناة تواصل بين جهاز الحاســب الآلي قيد التحقيق ومحطة التحليل الجنائي باستخدام بروتوكول التحكم بالنقــل (TCP)، ويتضمن هذا التطبيــق دالة المجموع الاختياري ودالة (MD٥) للتأكد من سلامة البينات، أما تطبيق (cryptcat) فهو النسخة المشفرة من تطبيق (netcat).

وأحد الأوامر الهامة هو أمر (systeminfo). ويوضح الشــكل (١٢-١٣) مخرجات الأمر (systeminfo) من جهاز حاسب آلي مكتبي يعمل على نظام ويندوز ٨. ومن المثير للاهتمام

أن هذا الأمر هو من الأوامر الأولى التي يقوم قراصنة الحاسب بتشغيلها في الجهاز المخترق وذلك لمعرفة مدى قوة الجهاز ومقدار المســاحة المتاحة. كما يحدد هذا الأمر التصحيحات التي تم تطبيقها على النظام.

قراصنة الحاسب والتصحيحات

ليس من المســتغرب أن يقــوم قراصنة الحاســب بتصحيحات للجهاز بعــد اختراقه. ويقوم قراصنة الحاســب بذلك ليس لأنهم طيبو القلــب بل حتى يضمنوا عدم وصول قراصنة آخرين إلى الجهاز نفسه.

وبشــكل عام فإن قراصنة الحاســب يفضلون أدوات ســطر الأوامر حتــى يتمكنوا من قراءة المخرجات وتقييمها من نظام آخر بســهولة. ومن الشــائع أن نجد ملفات السجل في مخرجات هذه الأدوات موجودة في حزمة واحدة وذلك عند التحقيق في حالة جهاز مخترق.

الشكل (١٢-١٣): مخرجات الأمر (systeminfo)

```
Command Prompt
Microsoft Windows [Version 6.2.9200]
(c) 2012 Microsoft Corporation. All rights reserved.

C:\Users\campo_000>systeminfo

Host Name:                 MALAZAN-CAMPOE
OS Name:                   Microsoft Windows 8 Enterprise
OS Version:                6.2.9200 N/A Build 9200
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          campoe@outlook.com
Registered Organization:
Product ID:                00178-50477-01524-AA453
Original Install Date:     1/16/2013, 10:50:03 AM
System Boot Time:          1/21/2013, 6:31:13 AM
System Manufacturer:       ASUSTeK Computer Inc.
System Model:              U46SM
System Type:               x64-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: Intel64 Family 6 Model 42 Stepping 7 GenuineInt
el ~800 Mhz
BIOS Version:              American Megatrends Inc. U46SM.203, 12/22/2011
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
```

استعادة الملفات:

يقوم قراصنة الحاســب بتوليد الســجلات. كما يملك قراصنة الحاســب بعض الأدوات التــي يقومــوا بنقلها إلى الأنظمــة المخترقة، متضمنــاً ذلك أدوات تشــخيص الأنظمة التي

ناقشـــناها ســـابقاً. وعادة ما يتم إزالة هذه الســـجلات والأدوات من النظام بمجرد البدء في عمليـــة التحقيق، لكن الحصول على مثل هذه الملفات يمثـــل إضافة كبيرة للتحقيق. وتُعد استعادة الملفات أمراً مفيداً خاصة في حالات التحقيق مع الأفراد، وحالات الاحتيال، وحالات الاستخدام غير النظامي لموارد المنظمة.

وهنـــاك فرق بين حـــذف الملـــف (deleting) ومحو الملـــف (erasing). وعادة يعتقد المســـتخدم أنه عند الضغط على زر الحذف (delete) في جهاز ويندوز فإنه سوف يتم إزالة الملف من النظام بشـــكل فعال. في حين أن هناك مســـتخدماً أكـــثر تطوراً يدرك أنه يجب «تفريغ سلة المهملات» حتى يتم إزالة الملف من النظام. لكن عدداً قليلاً من المستخدمين يُدرك أنه حتى عند الأخذ بهاتين الخطوتين لا يزال هناك إمكانية لاستعادة البيانات المرتبطة بهذا الملف.

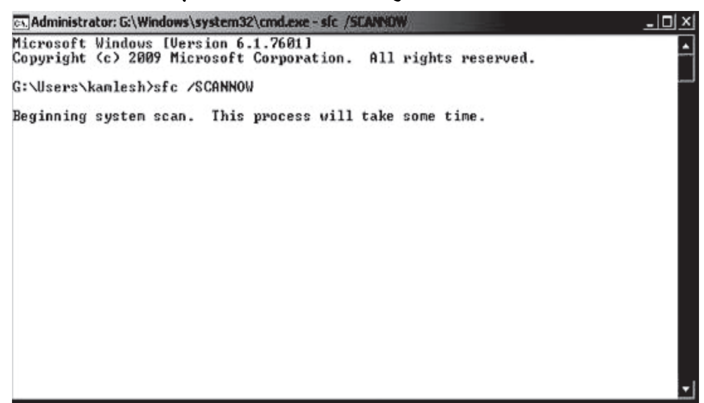
وهنا تبســـيط لعمليـــة حفظ ملف، فعندمـــا يتم حفظ الملف في جهاز الحاســـب الآلي فإنـــه يتم تقســـيم ذلـــك الملف إلى عدة أجـــزاء. يحتوي الجزء الأول عـــلى المعلومات التي تحـــدد مكان حفظ الأجزاء الأخرى على القرص (والتي يُشـــار إليها بـــ «واصفات البيانات» (metadata)). فعندمـــا يتم حذف الملف، يقوم نظام التشـــغيل بحذف الجزء الأول، وهو مـــؤشر العنوان، ويترك أجزاء البيانـــات الفعلية دون أن تُمس ويضـــع عليها علامة «صالحة للاستخدام» (usable).

ومن أجل تجنب فقدان البيانات يتم نسخ مؤشر العنوان في مواقع متعددة على النظام. فـــإذا تم إعادة بناء الجزء الأول اعتماداً على الأجزاء الاحتياطية قبل اســـتخدام الأجزاء التي وضع عليها علامة أنها متاحة، فإنه يمكن استرداد الملف بأكمله. وهناك طريقة أخرى لإعادة بناء الملف تُســـمى «نحت الملف» حيث تحاول هذه الطريقة إعادة إنشـــاء الملف اعتماداً على محتويات كل جزء من أجزاء الملف وليس اعتماداً على واصفات البيانات (metadata).

ويوضح الشـــكل (١٢-١٤) تشـــغيل أمر (System File Check) في جهاز بنظام تشغيل ويندوز ٨. ويتم تشـــغيل هذا الأمـــر عادة عند فقدان واصفـــات البيانات لملفات محددة وذلك عند تحميل نظام التشغيل.

اعتماداً على المحادثة الحالية، كيف يمكن محو الملف بشـكل فعال؟ إن أسـهل الطرق هي الكتابة على أجزاء البيانات بمحتويات عشوائية حيث تزيل هذه الطريقة المعلومات الحقيقية من جميع أجزاء البيانات مما يجعل استعادة الملفات غير ممكنة سواء باستخدام طريقة نحت الملفات أو غيرها. وللأسف فإن قراصنة الحاسب على علم بهذه المعلومة أيضاً.

الشكل (١٢-١٤): أمر (System File Check)



الأوقات الزمنية المرتبطة بالملفات (MAC times):

ناقشنا فيما سبق الأوقات الزمنية للأحداث التي وجدناها في جميع أنواع ملفات السجل. والآن سنتحدث عن الأوقات الزمنية المرتبطة بملفات البيانات.

تحتوي جميع الملفات، سـواء كانت في نظام ينكس أو نظام ويندوز، على ما لا يقل عن ثلاثـة أنواع من الأوقات الزمنيـة المرتبطة بتلك الملفات. وتعرف تلـك الأوقات الزمنية بـ (MAC times) وهي:

- وقت التعديل: ويشير إلى الوقت الذي تم فيه آخر تعديل على الملف.
- وقت الوصول: ويشير إلى الوقت الذي تم فيه آخر وصول أو قراءة للملف.
- وقت الإنشاء: ويشير إلى الوقت الذي تم فيه إنشاء الملف.

ووقت الوصول عادة ليس محل ثقة كبيرة لأنه يتغير غالباً. فماسـح الفيروسـات، على سـبيل المثـال، قد يقوم بالوصول إلى جميـع ملفات النظام يومياً، وذلـك أثناء البحث عن الفيروسـات. وتطبيق إلغاء تجزئة القرص يتمكن من الوصول إلى بقايا البيانات في الأقراص الصلبة، وذلك لتحسين الأداء عن طريق إزالة المساحات الفارغة بين البيانات. وكلا النشاطين السابقين يؤثر في وقت الوصول لملفات النظام. ويمكن تعطيل متابعة وقت الوصل بواسطة مسؤول النظام بهدف تحسين أداء نظام الملفات.

من جهة أخرى يتسـم وقت التعديل ووقت الإنشاء بموثوقية أكبر. وعلى الرغم من أن هذين الوقتين يمكن تغييرها برمجياً إلا أنها لا يمكن أن تُمس بواسطة قراصنة الحاسب.

دعنا نفترض أنه أثناء فحص سجل برتوكول (netflow) عثرنا على اتصال مشبوه باستخدام خدمة (ssh) في الخادم الذي نفحصه. هنا يسـتطيع سـجل برتوكـول (netflow) تحديد الوقت الزمني المرتبط بهذا الاتصال. كما يشير سجل برتوكول (netflow) إلى عدد كبير من الحزم التي يتم نقلها إلى الخادم، ويُلاحظ أن بعض الأحمال الحاسوبية انخفضت من النظام. لكن سـجل برتوكول (netflow) لا يستطيع أخبارنا بماهية الأحمال التي انخفضت. وحتى نعـرف ماهية الأحمال التي انخفضت لا بد من القيـام بفحص النظام. ويمكننا أن نفحص أدلـة الملفات واحداً بعـد آخر في محاولة لملاحظة ما هو خارج عن المألوف. لكن بدلاً عن ذلـك يمكننا بناء جدول زمني لملف الخادم ومن ثم تحديد الملفات التي أُنشـئت في وقت مقارب للوقت الذي عثرنا عليه في سجل بروتوكول (netflow).

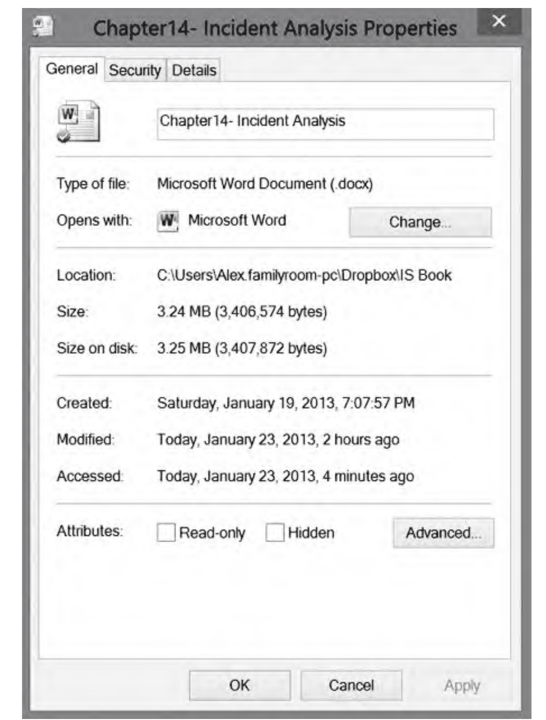
ويوضح الشكل (١٢-١٥) طريقة معرفة الأوقات الزمنية المرتبطة بالملفات (MAC times). ببسـاطة حدد الملف، ثم انقر بزر الفأرة الأيمن، ثم اختر خصائص (Properties). ويمكنك أيضـاً عرض التواريخ المختلفة المرتبطة بدليل كامل وذلك باسـتخدام مستكشـف الملفات وعرض العمود المناسـب، كما هو الحال في الشـكل (١٢-١٦). ويُعد ما ذكرناه آنفاً طريقة سريعـة لمعرفة الأوقات الزمنية المرتبطـة بالملفات في نظام قيد التشـغيل. لكن إذا كنت بحاجة لفحص القرص بالكامل فإنه من الأسهل استخدام أداة لفحص الأدلة بطريقة متكررة مثل أداة (mac_robber) أو غيرها من أدوات الأدلة الجنائية.

الجداول الزمنية:

بمجـرد الانتهاء مـن تجميع المعلومات فقد حان الوقت لبنـاء الجدول الزمني للحادث الأمني. وتشـكل الجداول الزمنية جزءاً أساسـياً من عملية التحليل. ويعد وضع الجداول الزمنية في أجهزة متعددة وربط تلك الجداول ببعضها البعض وربطها كذلك بسجل الشبكة جزءاً كبيراً من عمل الأدلة الجنائية.

ويوضح الشـكل (١٢-١٧) عينة لجدول زمني لخادم من خمسة خوادم كانت جزءاً من حادث أمني وقع في عام ٢٠٠٦. وكان التقرير الناتج يتكون من ١٥ صفحة، ويوضح التقرير أن الأنشـطة المشـبوهة في خادم (كينيا) كانت مؤكدة أيضاً في الخوادم الأخرى. والمسـح الذي بدأ في كينيا تم اكتشافه في خادم (أ) والعكس صحيح. وتم بناء الجدول الزمني كاملاً اعتماداً على فحص ملفات السجل المتنوعة في الخوادم الخمسة الأخرى.

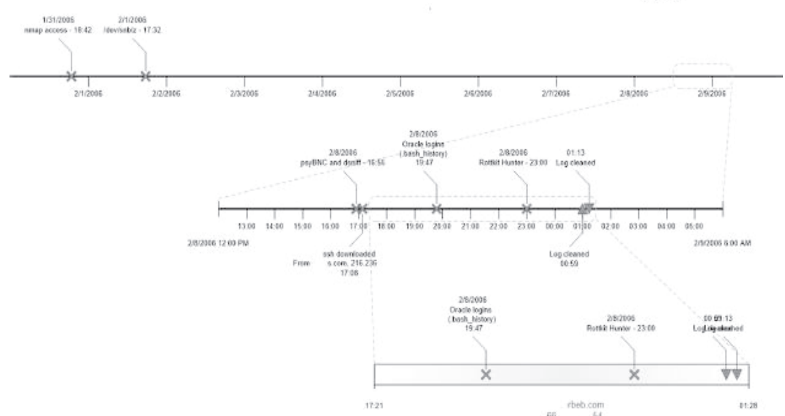
الشكل (١٢-١٥): الأوقات الزمنية المرتبطة بالملفات (MAC times)



الشكل (١٢-١٦): مستكشف الملفات بالأوقات الزمنية

Name	Date created	Date modified	Type	Size
Cache	1/19/2013 6:52 PM	1/19/2013 6:56 PM	File folder	
Cybersecurity Posters	1/19/2013 6:52 PM	1/19/2013 7:01 PM	File folder	
Final Drafts - Policies 2012 Revision	1/19/2013 6:52 PM	1/19/2013 6:56 PM	File folder	
Home Manuals	1/19/2013 6:52 PM	1/19/2013 7:17 PM	File folder	
IS Book	1/19/2013 6:52 PM	1/23/2013 5:44 PM	File folder	
ISW	1/19/2013 6:52 PM	1/19/2013 7:07 PM	File folder	
mSecure	1/19/2013 6:52 PM	1/19/2013 6:53 PM	File folder	
NotesPlus	1/19/2013 6:52 PM	1/19/2013 6:52 PM	File folder	
NUR3175 TO SHARE	1/19/2013 6:52 PM	1/19/2013 6:52 PM	File folder	
Perf Eval 2011	1/19/2013 6:52 PM	1/19/2013 6:57 PM	File folder	
Photos	1/19/2013 6:52 PM	1/19/2013 7:20 PM	File folder	
Public	1/19/2013 6:52 PM	1/19/2013 6:53 PM	File folder	

الشكل (١٢-١٧): عينة لجدول زمني



موضوعات ذات علاقة بأدلة التحليل الجنائي:

يعد موضوع أدلة التحليل الجنائي لتقنية المعلومات موضوع واسع للغاية ويحتاج فصل دراسي كامل لمناقشته، والمهارة تأتي فقط عن طريق الخبرة في هذا المجال. فالتدريب يجب أن يكون مستمراً لأن الأجهزة المحوسبة ذات القدرة الشبكية تتوسع باستمرار بدءاً من الهواتف الذكية ووصولاً لمنظمات الحرارة الذكية. والكثير من الأجهزة الإلكترونية المعقدة أصبحت «ذكية» وبدأت تأخذ جزءاً مهماً في العالم الذي نعيشه.

ويجدر بنا أن نذكر بعض التطورات الجديدة لأنها تجلب تحديات رئيسية لأدلة التحليل الجنائي. وأحد تلك التطورات هو التخزين في السـحابة الإلكترونية مثل التخزين من خلال تطبيق (Dropbox). ويعد هذا الموضوع جديداً على أمن المعلومات بشكل عام وأيضاً على أدلة التحليل الجنائي بشـكل خاص. على سبيل المثال، الملفات المحفوظة باستخدام تطبيق (Dropbox) يتم مشاركتها مع أجهزة حاسب آلي متعددة في شبكة حسابات (Dropbox). كـما أن الملفـات المحذوفة من مجلد (Dropbox) الموجود في جهاز الحاسـب الآلي لا يتم حذفها من البوابة الإلكترونية لـ (Dropbox)، ويمكن استعادتها بسهولة كما هو موضح في الشـكل (١٢-١٨). هل يستطيع المحقق الوصول لسـجلات (Dropbox)؟ وما مدى ذلك الوصول؟ وهل يتطلب ذلك مذكرة من المحكمة؟

الهواتف الذكية والأجهزة اللوحية الشـخصية تثير أيضاً بعض القضايا. ناقشـنا سـابقاً موضوع (أحضر جهازك الخاص) (BYOD) وهو اسـتخدام الموظف جهازه الشـخصي لأداء العمـل، وعادة يتضمن ذلك اسـتخدام بيانات مقيدة تملكها الشركـة. وتم تطوير أدوات أدلة التحليل الجنائي بحيث تسـمح للمحقق بتحليل صور القرص وتحليل ملفات الهواتف الذكيـة. ومعظم هذه الأدوات تعمل على نسـخ احتياطية مـن الجهاز وليس على الجهاز نفسـه. ويترتب على ذلك إما ملكية الجهاز من أجل إنشـاء نسـخ احتياطيـة أو إمكانية الوصول إلى النسخ الاحتياطية الموجودة. ومن ثم فإن التحقيقات الداخلية تكون في مأزق لأن الوصول إلى أحد هذه الخيارات يتطلب تعاون الموظف (والذي لا يتوافر في الغالب) أو مذكرة من المحكمة.

وبشـكل مشـابه لبقية موضوعات أمن تقنية المعلومات، فإن على أدلة التحليل الجنائي مواكبـة وتيرة التطور التقنـي. وفي كل مرة يكون هناك إصدار جديد لنظام التشـغيل، أو جهـاز جديد يحتوي على أنواع جديدة من ملفات النظام، فإن على أدوات التحليل الجنائي أن تتطور وتتكيف مع الوضع الجديد. وسـيكون هناك دائماً نوع من التأخر مما يسـتلزم عـلى المحققين أن يكونوا قادرين عـلى إيجاد البدائل والاجابـات الإبداعية عندما يتطلب الوضع ذلك.

الشكل (١٢-١٨): أمن المعلومات وإدارة المخاطر التقنية ليست مرعية من قبل شركة (Dropbox)

Dropbox

Adult Soccer League...py.jpg   Restore   Permanently delete   Previous versions

Name	Kind	Modified
11-036_062311_OASIS_FML.pdf	document pdf	6/23/2011 6:07 AM
100MEDIA$IMAG0800-1.jpeg	image jpeg	1/21/2013 10:55 AM
311083_127101267393662_100002813...75479_n.jpg	image jpg	10/17/2011 10:50 AM
.picasa.ini	file ini	2/16/2012 8:38 AM
.ynabSettings.yroot	file yroot	7/24/2012 7:13 AM
Adult Soccer League - FLYER - Copy.jpg	deleted image jpg	--
Adult Soccer League - FLYER.jpg	image jpg	2/16/2012 8:27 AM

نموذج حالة - اختراق الخادم الاحتياطي:

في أحد الأيام تم اختراق أحد أجهزة الحاسب الآلي في قسم تقنية المعلومات في الجامعة. وكان ذلك الجهاز يُستخدم كجهاز احتياطي لأنظمة التعامل مع البطاقات الائتمانية وكان الجهاز في طور إعادة البناء عندما تم اختراقه. ويُشتبه أن الاختراق تم من خلال استغلال ثغرة معروفة في نسخة قديمة لخادم قاعدة البيانات (MySQL) المثبتة في الجهاز. والسبب الرئيسي للقلق هو أن ملفاً هاماً يحتوي على بيانات حساسة قام قراصنة الحاسب بنقله من الجهاز قبل اكتشاف الاختراق. لكن نتيجة لسياسات المنظمة وتطبيق تلك السياسات، تم تشفير الملف بشكل كبير لذا لا يمكن قراءته من قبل قراصنة الحاسب دون معرفة المفتاح الخاص. ولا يعرف هذا المفتاح الخاص سوى شخصين داخل المنظمة.

والجدول الزمني للحادث مفيد جداً لأنه يوضح وتيرة الهجمات والحاجة للاستجابة السريعة من قبل تقنية المعلومات. وجميع الأحداث في الجدول التالي حدثت في يوم واحد.

الوقت	الحدث
الساعة ٨:٠٠ صباحاً	قام جهاز حاسب آلي بفحص بيانات الجامعة كما قام بجمع معلومات من خوادم (MySQL)، وعنوان بروتوكول الإنترنت لذلك الجهاز هو (١,٢,٣,٤)، كما أنه مسجل لـ (http://www.example.com) وموجود في مدينة تامبا بولاية فلوريدا.
الساعة١٠:٢١ صباحاً	كما قام جهاز حاسب آلي بعنوان بروتوكول الإنترنت (٢,٣,٤,٥) ومسجل لـ (Big ISP) في بلجيكا باختراق الجهاز المحلي بنجاح.

الساعة ١٠:٥٣ صباحاً	تم إنشـــاء بـــاب خفي عن طريق منفــذ (٣٠٠٠). وتم اســـتخدام هذا الباب الخفي لتشغيل برمجيات تشخيصية على الجهاز، كما تم نقل ملفات البيانات.
الساعة ١٠:٥٧ صباحاً	تم رفع الأدوات التشخيصية إلى الخادم بواسطة قراصنة الحاسب.
الساعة ١١:٠١ صباحاً	أول برنامج تشــخيصي هو (getallinfo.bat) وقد انتهى من مهمته حيث قام هذا البرنامج بتحديد قطع الأجهزة المادية على جهاز الحاسب الآلي بما في ذلك: سرعة وحدة المعالجة المركزية. مساحة القرص والذاكرة. قائمة بجميع التصحيحات المثبتة. قائمة بأحداث النظام المسجلة على الجهاز. قائمة مكتملة بجميع أجهزة الحاســب الآلي التابعــة لنفس النطاق الذي يتبع له الجهاز المخترق.
الساعة ١١:٠٣ صباحاً	ثاني برنامج تشــخيصي هو (speed.bat) وقد انتهى من مهمته حيث قام هذا البرنامج بجمع معلومات جديدة بما في ذلك: معلومات عن قطع الأجهزة المادية. قائمة بالعمليات الحالية التي تعمل على الجهاز. قائمة بالخدمات. معلومات عن المستخدم الذي قام حالياً بتسجيل الدخول.
الساعة ١١:١٤ صباحاً	الملــف الــذي يحتــوي عــلى معلومات حساســة عــن البطاقــات الائتمانية (datatodate.zip) تــم نقلــه من الجهاز. وهذا الملف مشــفر بشــكل كبير. والمفتاح الخاص اللازم لفك شــفرة الملــف ليس موجوداً في الجهاز المُخترق ولا يُعتقد بأنه تم اختراقه.
الساعة ١٢:٠٥ ظهراً	تــم اكتشــاف الاختراق وتــم إصدار تذكــرة بالموضوع. كما تــم التواصل مع المسؤول المحلي.
الساعة ١٢:٤٩ ظهراً	تم إعادة تشغيل الباب الخفي الخاص بنقل الملف من الخادم المخترق.
الساعة ١:٠٠ ظهراً	تم إزالة الجهاز عن الشبكة بواسطة المسؤول المحلي.

ويشير تثبيت خادم بروتوكول نقل الملفات (FTP) إلى أن قرصان الحاسب الذي اخترق الخادم كان ينوي جعل الخادم جزءاً من شــبكة من الأجهزة المخترقة التي تستخدم لتوزيع البرمجيات المقرصنة. وما يثير الدهشة هو أنه على الرغم من أن الهجمة لم تكن تستهدف الأجهــزة التي تحتوي على معلومات ماليــة، إلا أن المهاجم تمكن وبسرعة من تحديد مكان الملف الذي يحتوي على المعلومات الحساسة. ومع ذلك فإن المعلومات الموجودة في الملف المسروق ما زالت في أمان بسبب التشفير.

وتم استخلاص الدروس التالية وتطبيقها بعد تحليل هذا الحادث الأمني.

قائمة التحكم في الوصول:

قائمــة التحكم في الوصول هي خط الدفــاع الأول ضد الهجمات، وتم وضع هذه القائمة على الشبكة حيث تتحكم القائمة بالسماح للأجهزة بالوصول للخدمات في الأجهزة المستهدفة الأخرى.

تحديث خادم (MySQL):

ويبدو أن هذا هو مصدر الثغرة التي ســمحت لقراصنة الحاسب باختراق النظام. ومن ثــم فــإن تصحيح نظام التشــغيل فقط لا يحل جميــع القضايا الأمنيــة. ويجب أن يكون مســؤول النظــام المحلي على معرفة بجميع التطبيقات التي تعمــل على الجهاز، كما يجب عليه التعامل مع تحديثات الأمان الضرورية على وجه السرعة.

الخطوات الإضافية التي تم اتخاذها:

- مراجعة كاملة وشاملة للعمليات والإعدادات لضمان بيئة آمنة.
- تــم وضع برنامج لمراجعة قائمة الوصول لبروتوكــول الإنترنت (IP) ومراجعة وصول المستخدم الوظيفي للنظام وذلك لضمان الإدخالات الضرورية.
- تم إنشــاء أو تحديث الوثائق الهامة المرتبطة بالإجراءات الأمنية وخطط التعافي من الكوارث.

- تـــم إزالـــة المشـــاركة المفتوحة غـــير الضرورية والموجـــودة على الخـــوادم الإنتاجية والاحتياطية.
- لا يتم حفظ هذه الملفات على الخوادم، وإذا تم إرســـال شيء إلى أحد الموردين فإنه يتم حذفه على الفور.

أسئلة مراجعة للفصل:

١. ما تحليل الحوادث الأمنية؟ وما هدف تحليل الحوادث الأمنية؟

٢. ما تحليل السجل؟ وما هدف تحليل السجل؟

٣. افتـــح برنامج «عارض الأحـــداث» (Event Viewer) في جهـــازك. ما آخر الأحداث الموضحة في جانب «الأحداث الإدارية» (Administrative Events)؟

٤. ما الإدخال الأخير في جانب ملفات السجل التي تم عرضها مؤخراً؟

٥. ما المستويات المختلفة لأهمية السجل والتي يتم الإبلاغ عنها عادة بواسطة أنظمة ويندوز؟

٦. ما فائدة معلومات أهمية الحدث في سجل ويندوز؟

٧. ما المواقع الشائعة لملفات السجل في الأنظمة المعتمدة على نظام ينكس؟

٨. ما خدمة سجل النظام (syslog)؟

٩. ما محددات سجل النظام (syslog)؟

١٠. ما أجزاء محددات سجل النظام (syslog)؟

١١. ما سجل المصادقة في نظام ينكس؟ وما فائدته؟

١٢. ما ملف (wtmp)؟ وما فائدة المعلومات التي يحتويها هذا الملف؟

١٣. ما ملف (utmp)؟ وما فائدة المعلومات التي يحتويها هذا الملف؟

١٤. ما المعلومات التي يمكن الحصول عليها عادة من سجل خادم الشبكة؟

١٥. ما فوائد دمج السجلات؟

١٦.ما الاستجابة المباشرة للحوادث الأمنية؟ وما أهميتها؟

١٧.ما هي بعض المبادئ الأساسية للاستجابة المباشرة للحوادث الأمنية؟

١٨.لماذا تُعد الأوقات الزمنية مهمة في تحليل الحوادث الأمنية؟

١٩.ما الأوقات الزمنية المرتبطة بالملفات (MAC times)؟

٢٠.ما الجدول الزمني للحادث الأمني؟ وما فائدته؟

٢١.ما قضايا تحليل الحوادث التي تُثيرها خدمات التخزين في السحابة الإلكترونية مثل (Dropbox)؟

الأسئلة التالية تتعلق بتحليلك لجهاز حاسب الآلي مخترق تابع لأحد أعضاء هيئة التدريس. وقد عرفت أن هذا الجهاز تم اختراقه منذ ثلاثة أيام.

٢٢.ما الأداة التي يمكنك استخدامها لعرض سجل أحداث الجهاز؟

٢٣.ما الجانب الذي يحتوي على تاريخ إنشاء ملفات السجل؟

٢٤.ما الافتراضات التي يمكنك أن تطرحها إذا كان وقت انشاء كل من سجل التطبيقات، وسجل النظام، والسجل الأمني في الساعة الرابعة صباحاً؟

٢٥.هل هناك طريقة للحصول على تخمين منطقي حول آخر وقت استطاع قراصنة الحاسب الوصول فيه إلى الجهاز؟

أسئلة على نموذج الحالة:

١. كم الفترة الزمنية الفاصلة بين بداية المسح وسرقة الملفات التي تحتوي على معلومات البطاقات الائتمانية؟

٢. بافتراض أن هذه الهجمة لم يلاحظها أحد، ما الأضرار المحتملة التي يمكن أن تحدث في الجامعة؟

٣. ما الطرق التي يمكن أن تساعد في الإسراع في الكشف عن الحادث؟

نشاط التدريب العملي - تحليل سجل الخادم:

في هذا التدريب سنقوم بتحليل سجل الخادم من أحد خوادم الشبكة الإنتاجية.

وسنبدأ هذا التدريب بإلقاء نظرة على نسق السجل التالي:

```
[alice@sunshine ~]$ cd /opt/book/chptr_12
[alice@sunshine   ~]$ head -1 apache_
server.log
```

ونسق هذا الملف هو نسق (Apache) للسجل المركب ويتكون من الأعمدة التالية:

عنوان بروتوكول الإنترنت للعميل (مثلاً، ١٢٧,٠,٠,١).

هوية العميل وفقاً لحقل (inetd) - وفي الغالب يتم تعيين هذه القيمة «-» لهذا الحقل.

اســم المســتخدم للشــخص الذي يطلب البيانات إذا تم اســتخدام مصادقة بروتوكول (HTTP)، أما إذا لم يتم استخدام المصادقة، فإن قيمة هذا الحقل ستكون «-».

وقت معالجة الطلب (مثلاً، [0500-Jan/2013:10:14:02/16]).

طلب بروتوكول (HTTP) المرسل من العميل (مثلاً، «GET/images/gtalk.png HTTP/1.1»).

رمز الحالة لبروتوكول (HTTP) (مثلاً، ٢٠٠).

حجم البيانات المرسلة بالبايت (مثلاً، ١٥٠٦).

«المرجع» وهو الصفحة التي توجه العميل لطلب هذا المورد (http://www.sunshine.edu/).

«وكيل المستخدم» والذي يعطيك معلومات عن متصفح الشبكة ونظام التشغيل المستخدم من قبل العميل («Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.0)»).

مــن بين هــذه الحقول يجب أن نهتم ببعــض منها فقط. وســوف نناقش أهمية تلك البيانات كما ســنوضح كيفية اســتخراجها باســتخدام الأمر (cut) والذي تعلمناه في الفصل العاشر.

عنوان بروتوكول الإنترنت (IP) للعميل:

إذا كان هنــاك حادث مُحتمــل، يجب عليك أن تعرف من أيــن أتى العميل. ملاحظة: هذه المعلومات مستخرجة من أحد خوادم الشبكة الإنتاجية، وتم تعديل عناوين بروتوكول الإنترنت لحماية خصوصية المستخدم.

```
[alice@sunshine ~]$ head -4 apache_server.
log | cut -d«» -f1
YX.224.59.134
YX.224.59.134
YYP.63.193.132
YAY.247.53.103
```

الوقت الزمني:

أهميــة الوقت الزمني تعادل أهمية عنوان بروتوكــول الإنترنت لأنك تحتاج إلى معرفة وقت تقديم الطلب إلى خادم الشبكة.

```
[alice@sunshine ~]$ head -4 apache_server.
log | cut -d« » -f4,5
[16/Jan/2013:10:13:55 -0500]
[16/Jan/2013:10:13:55 -0500]
[16/Jan/2013:10:13:56 -0500]
[16/Jan/2013:10:13:58 -0500]
```

طلب بروتوكول (HTTP):

١. طلب بروتوكول (HTTP) مقسم إلى ثلاثة أجزاء:

٢. الطريقة: يستخدم الأمر (GET) لطلب البيانات، ويستخدم الأمر (POST) لإرسال البيانات.

٣. الموارد التي يتم طلبها (صفحة HTML، صورة، نص PHP، وغيرها).

٤. إصدار بروتوكول (HTTP) المستخدم، وعادة يكون الإصدار (HTTP/1.1).

```
[alice@sunshine ~]$ head -4 apache_server.
log | cut -d« » -f6,7,8
«GET /favicon.ico HTTP/1.1»
«GET /favicon.ico HTTP/1.1»
«GET / HTTP/1.1»
«GET / HTTP/1.1»
```

رمز الحالة لبروتوكول (HTTP):

وهو الرمز الذي يرسله الخادم إلى العميل. «هذه المعلومات قيمة جداً لأنها تكشف ما إذا أدى الطلب إلى استجابة ناجحة (الرموز تبدأ بالرقم ٢)، أو إلى إعادة توجيه (الرموز تبدأ بالرقم ٣)، أو إلى خطأ بسبب العميل (الرموز تبدأ بالرقم ٤) أو إلى خطأ في الخادم (الرموز تبدأ بالرقم ٥)»[٢].

```
[alice@sunshine ~]$ head -4 apache_server.
log | cut -d« » -f9
404
404
200
200
```

(2) http://httpd.apache.org/docs/1.3/logs.html

وكيل المستخدم:

سلســلة رموز وكيل المســتخدم توفر معلومــات هامة عن العميل مثــل نوع المتصفح واصــداره وكذلك إصدار نظام التشــغيل. ملاحظة: تم توليد سلســلة الرمــوز التالية من متصفــح العميل ويمكن تعديلها. لذا لا تفترض أن هذه البيانات صحيحة (١٠٠٪). وعادة ما تستخدم سلســلة الرموز هذه في تحليل الاستخدام العام مثل تحديد نسبة المستخدمين الذين يصلون إلى صفحة الشبكة من خلال الأجهزة المحمولة.

```
[alice@sunshine ~]$ head -4 apache_server.
log | cut -d'«' -f6
Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:21.0) Gecko/20130115
Firefox/21.0
Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:21.0) Gecko/20130115
Firefox/21.0
Mozilla/4.0 (compatible; MSIE 7.0; Windows
NT 6.0)
Mozilla/5.0 (Macintosh; U; Intel Mac OS X
10_6_8; en-us)
AppleWebKit/533.21.1 (KHTML, like Gecko)
Version/5.0.5 Safari/533.21.1
```

لاحظ أننا اســتخدمنا علامة الاقتباس (' « ') بدلاً من المســافة (' ') كمحدد للأمر (cut) حيث يحتوي وكيل المســتخدم على عدد من المتغيرات مفصولة بمســافات، لكنها دائماً تبدأ وتنتهي بعلامة اقتباس مما يجعل علامة الاقتباس محدداً أكثر موثوقية.

أسئلة:

للإجابة عن الأسـئلة التالية، استخدم المعرفة التي اكتسبتها في استخراج بيانات الملفات باسـتخدام الأوامر (grep)، والأمر (sort)، وغيرها من الأوامـر التي تعلمتها في التدريبات العملية في هذا الكتاب:

١. كم عدد عناوين بروتوكول الإنترنت (IP) التي أرسلت طلبات؟

٢. ما عنوان بروتوكول الإنترنت (IP) الذي أرسل أكثر الطلبات؟ هل كانت تلك الطلبات ناجحة؟ وكيف عرفت ذلك؟

٣. ما وكيل المستخدم الأكثر شيوعاً؟

٤. كم عدد وكلاء المسـتخدم الموجودة في كلمـة (iPad) أو كلمة (iPhone) في مقابل كلمة (Android)؟

٥. لقـد تـم إعلامـك للتـو أن هناك نشـاطاً مشـبوهاً عـلى جهـاز ما في الشـبكة (YAY.247.114164). أنشـئ قائمـة بجميع الموارد (إن وجـدت) والتي تم طلبها باستخدام هذا النظام.

٦. تـم اخـتراق خادم ويب آخـر في الحرم الجامعـي من خلال ثغـرة أمنية في أدوات المسـؤول المعروفة بـــ (wp-admin) والتابعة لمدونة تطبيـق (Wordpress). ولم تتمكـن من معرفة عنوان بروتوكول الإنترنت (IP) الذي اسـتخدمه المهاجم، لكنك تتوقع قيام المهاجم بمسح خوادم ويب أخرى للعثور على ثغرات في (Wordpress). ابحث في سـجل خادم الشـبكة لمعرفة إذا ما تم أي مسـح للخـادم، وحدد عنوان بروتوكول الإنترنت (IP) الذي ينشأ منه ذلك المسح.

تمرين التفكير النقدي - الهدم في إدارة التنمية الاقتصادية:

نسبة كبيرة من تحليل الحادث في إدارة التنمية الاقتصادية (EDA) تمت بواسطة متعهد خارجي. وفيما يلي جزء من تقرير مكتب المفتش العام (OIG) حول هذا التحليل:

بعد أسـبوعين من بداية أنشـطة الاسـتجابة للحادث الأمني اكتشف المتعهد الأمني في إدارة التنميـة الاقتصادية أن المؤشرات الأولية لوجود برامـج ضارة دائمة إنما هي مؤشرات إيجابية خاطئة - أي لا يوجد انتشـار حقيقي للبرمجيات الضارة. لكن مدير المعلومات في إدارة التنمية الاقتصادية سـعى لضمان التأكد من خلو الأجهزة من البرمجيات الضارة، كما سعى للتأكد من عدم اسـتمرارية وجود تلك البرمجيات. لكن المتعهد الخارجي للاستجابة للحادث الأمني لم يتمكن من تقديم الضمان الذي يسعى إليه مدير المعلومات، لأن تقديم ذلـك الضمان ينطوي على إثبات أن الإصابة بالبرمجيات الضارة لا يمكن أن تحدث بدلاً من إثبات أنها لم تكن موجودة. وبحلول السـادس عشر من إبريل من عام ٢٠١٢، وعلى الرغم من مرور أشهر من البحث، لم يتمكن المتعهد الأمني في إدارة التنمية الاقتصادية من العثور عـلى أي برمجيـات ضارة دائمة أو على مؤشرات هجمات تسـتهدف أنظمـة إدارة التنمية الاقتصاديـة. وعلاوة على ذلك فـإن وكالة الأمن القومي الأمريكيـة (NSA) وكذلك مركز استجابة طوارئ الحاسب الآلي الأمريكي (US-CERT) لم يعثرا على أي أنشطة دولية أو أي برمجيات ضارة دائمة.

- هـل تتفق مع معيـار الأمان الذي يسـعى له مديـر المعلومـات في إدارة التنمية الاقتصادية - ضمان عدم وجود البرمجيات الخبيثة في أنظمة المنظمة؟
- اعتماداً على هذا التقرير، ما رد فعل المتعهد الأمني على هذه النتائج؟

تصميم حالة:

فيـما يلي ملخص لتحليل حادث أمني قمـت بالتحقيق فيه والذي وقع في وحدة تقنية المعلومات المركزية.

تم اختراق خادم (APPSERVER١) في مسـاء التاسـع والعشرين مـن فبراير من عام ٢٠١٣. وتمكن قراصنة الحاسـب من الوصول للجهاز لمدة ساعة. وخلال هذا الوقت حاول قراصنة الحاسب الوصول إلى أجهزة أخرى في شبكة جامعة ولاية الشمس المشرقة باستخدام مجموعة من ستة بيانات اعتماد مختلفة.

وتم استخدام أساليب التحقيق التالية لتحديد مدى الاختراق:

- استخدام واسع لأدلة التحليل الجنائي بما في ذلك أداة (Autopsy) وأداة (Sleuthkit) لتحديد الجدول الزمني للأحداث، وتحديد موقع ملفات السجل واستخراجها، وتحديد الأبواب الخفية، ومسجل المفاتيح (key loggers).
- تمت استعادة سجل أحداث ويندوز كما تم فحصه بالتفصيل.
- تم كذلك فحص اتصالات الشبكة الواردة إلى خادم (APPSERVER1) والصادرة منه.
- تم الاهتمام بحركة المرور الواردة لخادم قاعدة البيانات (DBI) والصادرة منه لأن هذا الخادم يحتوي على بيانات شخصية مقيدة في الجامعة.

استخدم قراصنة الحاسب كلمة سر معروفة للوصول إلى تطبيق (Remote Desktop) في واجهة خادم (APPSERVER1). وكشفت المزيد من التحقيقات عن قائمة من بيانات الاعتماد المخترقة سابقاً. واتضح أن بيانات الاعتماد التي استخدمها قراصنة الحاسب للوصول إلى خادم (APPSERVER1) هي الوحيدة التي كانت سارية المفعول في ذلك الوقت حيث تنتهي صلاحية كلمات المرور في الجامعة خلال ١٨٠ يوماً.

الجدول الزمني:

٢٠١٣/٢٩/٢ الأحد الساعة ٧:٣١ مساءً	مؤشرات أولية للاختراق، تم استخراجها من سجل تدفق الشبكة. اتصال من خارج الحرم الجامعي من (٦٧,١٠٥,١٣٨,١٩٤) باستخدام تطبيق (Remote Desktop) والمسجل في شركة (XO Communications) والمملوكة لشركة (Peaks and Plains Medical) في مدينة سبوكين بولاية واشنطن.
٢٠١٣/٢٩/٢ الأحد الساعة ٧:٣٧ مساءً	تم إعادة تشغيل الجهاز في محاولة لبدء عملية تنصت من خلال باب خفي على منفذ (١٠٣٤). ويتم ذلك من خلال خوادم بروتوكول نقل الملفات، أو قنوات تحكم آلية تسمح للمستخدم البعيد بالسيطرة على الأجهزة المحلية دون الحاجة لاستخدام تطبيق (Remote Desktop). وتم استدعاء المسؤول في جامعة ولاية الشمس المشرقة بسبب إعادة التشغيل غير المجدولة.

٢٠١٣/٢٩/٢ الأحد الساعة ٧:٣٩ مساءً	حاول قراصنة الحاسب الاتصال بأجهزة أخرى في الجامعة، لكن محاولاتهم باءت بالفشل.
٢٠١٣/٢٩/٢ الأحد الساعة ٨:٤٢ مساءً	قام قراصنة الحاسب بتسجيل خروج من النظام. ولم يتم اكتشاف أي محاولات أخرى لتسجيل الدخول.

أسئلة:

١. متى تم اكتشاف الحادث الأمني؟ وكيف تم ذلك؟

٢. ما المعلومات الهامة الناقصة؟

٣. اعتماداً على ما تعرفه، ما الأمور التي ستنتظر اليها للوصول إلى فهم أفضل للنتائج النهائية للحادث الأمني؟ اذكر التفاصيل قدر المستطاع.

٤. ما مقترحاتك لتطوير الوضع الحالي؟

الفصل الثالث عشر

السياسات والمعايير والمبادئ التوجيهية

نظرة عامة:

في الفصول السابقة ألقينا نظرة واسعة على التحديات والمخاطر التي تواجه المنظمات التي تعتمد أعمالها على شبكات البيانات. وجميع المنظمات، سواء كانت منظمة حكومية أو منظمة خاصة، تواجه تحديات أمنية متشابهة تتمثل في معرفة أفضل السبل لحماية الأصول دون إضعاف الإنتاجية ودون التأثير على المحصلة النهائية للمنظمة. كما ناقشنا في الفصول السابقة التدابير الوقائية المختلفة لحماية الأصول والتي يقوم بتأديتها مسؤولو النظام المدربون. كما ناقشنا فيما سبق الإجراءات الموصى بها للتفاعل مع الأحداث السلبية ومن ثم السيطرة على الأضرار والتقليل من تأثيرها في المنظمة.

في هذا الفصل سنبتعد قليلاً عن العالم التقني وسنناقش الآليات الإدارية المتاحة للمحلل الأمني ومسؤول النظام. فالمحلل الأمني يمكنه توجيه سلوك مستخدمي تقنية المعلومات في المنظمة بطريقة تقلل من المخاطر الأمنية بما تتيحه له مثل هذه الآليات. وبدون هذه الآليات فإن مسؤول النظام سيقضي وقتاً طويلاً جداً لإصلاح المشكلات الأمنية التي يفترض ألا تحدث في المقام الأول مما يسبب تكاليف كبيرة على المنظمة.

في نهاية هذا الفصل يجب أن تكون قادراً على:

- فهم الفرق بين المتطلبات الأمنية ومتطلبات الامتثال.
- التمييز بين السياسات والمعايير والإجراءات.
- فهم دورة حياة السياسات.
- تحديد مجموعة من السياسات التي تُعد ضرورية لأي منظمة.

الأسس التوجيهية:

الآليات الإدارية المستخدمة في الصناعة لتوجيه سلوك المستخدم هي السياسات، والمعايير، والمبادئ التوجيهية. وتسمح هذه الآليات للمسؤول عن أمن المعلومات بالحصول على مصادقة المسؤولين في المستوى التنفيذي لأهداف أمن المعلومات داخل المنظمة وترجمة هذه الأهداف إلى بنود قابلة للتنفيذ ومحددة لجميع أعضاء المنظمة. وعندما تشير خبرات تلك الآليات في التعامل مع الحوادث الأمنية إلى مسؤولي الأمن أن المنظمة تحتاج إلى تغيير الطريقة التي تتعامل بها مع أمن المعلومات، فإنها تلفت انتباه الإدارة العليا للقيام بمراجعة شاملة بناء على التغييرات المقترحة. وبينما تهتم الإدارة العليا بأمن المعلومات، فإنها تدرك كذلك أن إضافة المزيد من الأمن يعيق عادة العمل، كما يمكن أن يضيف ذلك تكاليف تدريب كبيرة للتعامل مع هذا التغيير. لكن إذا كان هناك ما يُبرر التغيير فإن الإدارة العليا ستسمح بذلك التغيير. ويتم نشر ممارسات أمن المعلومات الناتجة على شكل سياسات، أما المعايير والمبادئ التوجيهية فإنها تنبثق من تلك السياسات. ويجب أن تكون السياسات، والمعايير، والمبادئ التوجيهية موجهة، كما يجب أن يكون لها أهداف واضحة. ولتحقيق ذلك فإنه من الضروري فهم المبادئ الأساسية لأمن المعلومات والمهمة لدى المنظمة، واستخدام تلك المبادئ كدعم حقيقي للسياسات. وسنُناقش بعضاً من تلك المبادئ في الفقرات القليلة القادمة.

أولاً وقبل كل شيء، على المنظمة استيعاب حقيقة أن أمن المعلومات يؤثر في المنظمة وموظفيها وعملائها ويكون ذلك التأثير على أساس يومي. أمن المعلومات ليس شيئاً تفعله اليوم وتتركه غداً وترجع له مرة أخرى الأسبوع القادم، فالمبادئ السليمة لأمن المعلومات يجب أن تكون جزءاً لا يتجزأ من جميع أنشطة المنظمة.

وبعد ذلك ينبغي إدراك مفهوم «طبقات الأمن». وبالنسبة للمشكلات الأمنية، لا يوجد حل يتصف بأنه «مقاس واحد مناسب للجميع». وبصفتك محللاً أمنياً أو مسؤولاً للنظام ستجد العديد من الشركات التي تحاول إقناعك بأن منتجاتها لا غنى عنها على الإطلاق وأن تلك المنتجات تحل جميع المشكلات الأمنية. وهذا ليس صحيحاً إطلاقاً. إذا كان ذلك صحيحاً، فإننا لن نرى في وسائل الإعلام حالات متكررة لانتشار الفيروسات، وتسرب البيانات

وهجمات الشـبكات. والحل الأمثل للرد عـلى القراصنة والبرمجيات الخبيثة والمحتالين هو تطبيـق أنظمة أمنية متعددة من أجل حماية أصول المنظمـة. ولحماية البيانات في خادم الملفات بإمكانك تطبيق نظام تسـجيل دخول بكلمات مرور معقدة، وباستخدام القياسات الحيوية، وجدار ناري، وحماية نقطة النهاية، والتشفير، على أمل أن واحداً من هذه الأنظمة سيكتشف أي نشاط يهدد المنظمة.

كما أن فهم مواقف المنظمة الأخرى يسـاعد في كتابة السياسـات. فهل تفضل المنظمة البرمجيات مفتوحة المصدر أم البرمجيات التجارية؟ الخيارات المختلفة قد تؤدي إلى اختلاف في متطلبات السياسات. وهل تعتمد المنظمة على معايير صناعة واحدة في جميع الحالات، أم أن المنظمة انتقائية في المعايير التي تعتمد عليها؟ وهل تُوظف المنظمة مستشارين على أساس مؤقت، أم أنها تسعى للحفاظ على المعرفة داخل المنظمة؟

السياسات:

وفقاً لنموذج (أهـداف التحكم للمعلومات والتكنولوجيـا ذات الصلة) (COBIT)[1]، «السياسـات هي وثيقة تُسـجل مبادئ رفيعة المستوى أو مسـار العمل الذي تم إقراره». والتركيز هنا على «رفيعة المستوى» لأن السياسات تعكس مبادئ تم تأييدها من مستويات عاليـة في المنظمـة. ويُعد وقت المديريـن التنفيذيين في هذا المسـتويات مُكلف جداً، لذا يبذل هؤلاء المُديرون جهدهم في عدم إعادة النظر مرة أخرى في القضية نفسها. وبناء على ذلك تكون السياسات مكتوبة بلغة عامة للتعامل مع التطورات الروتينية في مجال الأعمال والتقنية. أما الآليات الإدارية الأخرى: المعايير، والمبادئ التوجيهية، والإجراءات؛ فإنها تنبع من السياسـات وتقدم إلى جميع الموظفين توجيهات محـددة وقابلة للتنفيذ. ويتم كتابة المعايير، والمبادئ التوجيهية، والإجراءات بواسـطة خبراء مثل مسؤول النظام، ومن ثم يمكن أن تتغـير وفقـاً للتغييرات التنظيمية. وبينما تحدد السياسـات الاتجـاه العام الذي يجب على المنظمة اتباعـه، دون الاهتمام بكيفية الوصول إلى ذلك الاتجاه، فإن المعايير، والمبادئ التوجيهية، والإجراءات تركز على كيفية الوصول للاتجاه الذي ترغب فيه السياسات.

---

(1) COBIT 5 Glossary, http://www.isaca.org/Knowledge-Center/Documents/Glossary/glossary.pdf

على سـبيل المثال، تنص سياسة الاسـتخدام الملائم لأرقام الضمان الاجتماعي (SSN Appropriate Use Policy)[٢] رقم (516-0) في جامعة جنوب فلوريدا على ما يلي:

يتم التخلص من الملفات الورقية والإلكترونية التي تحتوي على أرقام الضمان الاجتماعي بطريقة آمنة وفقاً لسياسات الاحتفاظ والتخلص التابعة للولاية والدولة.

ولا يوجـد تفاصيـل حول كيفية التخلص مـن الملفات الورقية التـي تحتوي على أرقام الضـمان الاجتماعـي. الشرط الوحيد هو أن يتم ذلك «بطريقة آمنة» وفقاً للقانون. وتُركز السياسـة على التخلص من تلك السـجلات، وليس على كيفية تنفيذ ذلك، لأن ذلك يعتمد على التكنولوجيا المتاحة، والتكلفة، وغيرها، كما سـيتم توضيحه من خلال المعايير، والمبادئ التوجيهية، والإجراءات.

المعايير:

المعيـار هـو مجموعة محددة مـن القواعد المقبولـة والمعتمدة من قبـل العديد من المنظمات. ويشـار إلى بعـض المعايير بأنها «معايير الصناعة»، وهي الأنشـطة والإعدادات والقياسات المقبولة من جميع المنظمات في صناعة معينة، ويبغي أن ينظر إليها بأنها مبادئ العمليات.

ويُعـد المعهد الوطني للمعايـير والتكنولوجيـا (National Institute for Standards and Technology)، والـذي يعـرف اختصاراً بـ (NIST)، أحد مصـادر أهم معايير تقنية المعلومات، على الأقل بالنسـبة للمنظمات داخل الولايات المتحدة الأمريكية. وعلى الرغم مـن أن وثائق المعهد الوطنـي للمعايير والتكنولوجيا تُصنف بأنهـا «توصيات» أو «مبادئ توجيهيـة»، إلا أنها تُعد في الواقع معايير لجميع المنظـمات في الولايات المتحدة الأمريكية. وقد استعرضنا بعض الأمثلة في هذا الكتاب ومن ذلك «المبادئ التوجيهية لتقييم المخاطر».

كـما تُعـد المنظمـة الدوليـة للمعايـير (International Organization for Standardization) والمعروفـة اختصـاراً (ISO) منظمـة أخرى مقبولـة في جميع أنحاء

(2) SSN Appropriate Use Policy, University of South Florida, http://generalcounsel.usf.edu/policies-and-procedures/pdfs/policy-0-516.pdf

العـــالم لبنـــاء معايير بأســـس دولية. وأحد معايـــير (ISO) الأكثر اســـتخداماً هو معيار رقـــم (27002/17799) وهو المعيار التابع لأمـــن المعلومات. ووفقاً لموقع (ISO) على الإنترنت، فإن هذا المعيار «يؤســـس المبـــادئ التوجيهية والمبادئ العامة لبدء إدارة أمن المعلومـــات في المنظمة وتطبيقها والحفاظ عليها وتطويرها. أما الأهداف المحددة فهي تقدم إرشـــادات عامة للأهـــداف المقبولة عموماً في إدارة أمـــن المعلومات». ويتضمن معيـــار (ISO/IEC 27002:2005) أفضل الممارســـات المتعلقة بأهـــداف التحكم وأهداف المجالات التالية من إدارة أمن المعلومات:

- السياسات الأمنية.
- تنظيم أمن المعلومات.
- إدارة الأصول.
- أمن الموارد البشرية.
- الأمن المادي والأمن البيئي.
- إدارة العمليات والتواصل.
- التحكم في الوصول.
- اقتناء نظم المعلومات وتطويرها وصيانتها.
- إدارة حوادث أمن المعلومات.
- إدارة استمرارية العمل.
- إدارة الامتثال.

وبمجرد قبول المعايير في المنظمة فإنها تكون الزامية. على سبيل المثال، من أجل أن تعلن المنظمة بأنها متوافقة مع معيار (ISO 27002) يتعين عليها الالتزام بجميع اللوائح المرتبطة بهذا المعيار حيث لا يوجد شيء يسمى بـ «الامتثال الجزئي».

فـي عـام ٢٠٠٩، وضعت شـركة (Symantec) ملصقاً مصمماً بطريقة جيـدة يعرض معايير متطلبـات الامتثال المختلفـة، وذلك بطريقة واضحة بحيث يمكن للقارئ أن يحدد بسـرعة أوجه التشـابه بين كل فئة من المتطلبات الأمنية. ويمكن الاطلاع على نسـخة من الملصق على هذا الرابط:

http://net.educause.edu/ir/library/pdf/CSD5876.pdf

كـما أن للمعايـير علاقة مباشرة بالسياسـات. على سـبيل المثال، يمكن للسياسـات أن تـصرح بأنه يجب تثبيت حلول حماية نقطة النهاية (EPP) المطروحة من قبل إدارة تقنية المعلومـات والمتاحة على الموقع الإلكتروني التابع لها، وذلك في جميع أجهزة الحاسـب الآلي في المنظمة. وبعد ذلك يقوم المعيار بتحديد حلول حماية نقطة النهاية التي يجب تثبيتها. والميزة في هذه الحالة واضحة. وكما سنرى أن السياسات عادة تكون أصعب في التعديل من المعيار. فمن خلال السـماح لإدارة تقنية المعلومات بالاحتفاظ بمعيار حماية نقطة النهاية (EPP) فإن السياسات تسمح لإدارة تقنية المعلومات باتخاذ القرارات ذات العلاقة بحماية نقطـة النهاية (EPP) دون الحاجة لتحمل عبء المرور بالدورة الكاملة لحياة السياسـات والموافقة عليها.

وأخـيراً فإن المعايير تجعل السياسـات أكثر وضوحاً. وبالنظـر إلى المثال الذي ذكرناه في الفقرة السـابقة، فإن حماية نقطة النهاية (EPP) تكون غامضة بدون معيار. حماية نقطة النهاية هي عبارة عن مجموعة من التطبيقات التي تحمي الجهاز، وتحتوي عادة على حلول لمكافحة الفيروسات، كما تحتوي على الحلول الاختيارية التالية:

- اكتشاف التسلل المعتمد على المضيف.
- الجدُر النارية.
- جدولة مسح الفيروسات أو مسح المنافذ في الوقت الفعلي.
- تقييم الثغرات.
- سمعة الموقع الإلكتروني.

بــدون المعايير يكون لــدى المنظمة مزيج مــن الحلول. فالمعايير تحــدد أي من هذه الخيارات مهمة للمنظمة ومن ثم تُجبر جميع الوحدات على تنفيذ تلك الحلول.

المبادئ التوجيهية:

المبــادئ التوجيهية هي الإجراءات التي توجه إلى الوحدات لتطوير العمل عندما تكون الأمور تســير بطريقة معينة، لكن تلك الإجراءات ليســت شرطاً لذلك. على ســبيل المثال، لنفترض أن هناك تطبيقاً جديداً لمكافحة الفيروسات يعمل على نظام (iOS)، وهذا التطبيق يعمل بشــكل رائع. وبناء على ذلك قد «تقترح» إدارة تقنية المعلومات أن على كل شخص تثبيــت وتشــغيل هذا التطبيق، لكــن بدون وجود سياســات تفيد بأن لــدى إدارة تقنية المعلومات القدرة على القيام بذلك، فإن هذا الاقتراح يكون خيارياً ولا يكون إلزامياً.

وقد تتطور بعض المبادئ التوجيهية لتصبح معايير في وقت لاحق. وبدون إدارة مركزية لتقنيــة معلومات في البيئة الجامعية قد يكون من الصعب على المنظمة الأمنية دعم حلول موحدة لمكافحة فيروســات. وهذا قد ينطوي عــلى إقناع جميع الوحدات على التخلي عن حقها في تشــغيل برنامج مكافحة الفيروســات الذي يعجبها. وبدلاً من ذلك فإن إدارة أمن المعلومات قد تضطر لوضع مبادئ توجيهية تحدد فيها التعامل مع المورد (أ) والأسباب التي أدت إلى ذلك.

وعندما تكون الأســباب سياسية أكثر من كونها أسباب فنية، فإن استخدام مبدأ «الجزرة مقابل العصا» مفيد للغاية في هذا الســيناريو. فإذا كانت إدارة امن المعلومات قادرة على توفــير البرمجيات من خلال المورد (أ) مجاناً لجميع الوحدات في الحرم الجامعي فإن الكثير من الوحدات ستجد الفكرة جذابة وستقوم باستخدام البرنامج. وهذا هو منهج الجزرة.

والنقطة الأساسية في هذا القسم أن المبادئ التوجيهية يتم اعتمادها في حدود ضيقة وعلى أســاس تطوعي. وسيستمر اســتخدام الوثيقة الناتجة على أســاس أنها مبادئ توجيهية حتى يكون هناك سلطة كافية ممنوحة من الإدارة لجعل الوثيقة من ضمن المعايير (الشكل ١٣-١).

الشكل (١٣-١): السياسات والمعايير والمبادئ التوجيهية



لماذا نحتاج إلى الكثير من العمل المكتبي؟

شكوى تقليدية تصدر من الموظفين الفنيين وهي «لماذا علينا أن نتحمل كل هذا العناء؟» و«لماذا نحتاج إلى الكثير من العمل المكتبي؟» موظفي تقنية المعلومات هم أشخاص عمليين، ومن ثم فإن التوثيق ليس نقطة من نقاط قوتهم. لكن الحاجة إلى الحفاظ على السياسات تتجاوز الامتثال. إن توثيق هذه العمليات بالشكل الصحيح لا يقوم فقط بإضافة الروتين والبيروقراطية، بل يمكن أن يساعد في تحسين أداء المنظمة.

على سبيل المثال، السياسات الأمنية مؤشر للعملاء والمستخدم النهائي وحتى الموظفين بأن المنظمة تتعامل مع الأمن على محمل الجد. مثلاً، تتضمن السياسة الأمنية لمدينة تامبا بولاية فلوريدا ما يلي:

الاستخدام الآمن للإنترنت يحظى بأولوية عالية في مدينة تامبا. ونحن ندرك بأن أمن المعلومات له أهمية قصوى بالنسبة لك، لذا خصصنا الكثير من الجهد لضمان الحفاظ على معلوماتك الشخصية[٣].

وتشير هذه السياسة إلى الأهمية التي توليها المنظمة لأمن المعلومات، والتي يجب أن تكون مطمئنة للمستخدمين المعنيين. كما تقدم السياسات خارطة طريق للموظفين والمستخدمين الجدد.

---

(٣) سياسة الانترنت لمدينة تامبا، http://www.tampagov.net/about_us/tampagov/internet_policies/security_policy.asp

وأحد السياســات الشائعة التي ســنراها في الأجزاء القليلة المقبلة تُعرف باسم «سياسة الاستخدام المقبول» (acceptable use policy) أو اختصاراً (AUP). وتصف هذه السياسة للمستخدمين أوامر ونواهي النظام، أو الأشياء المقبول القيام بها والأشياء التي من شأنها أن تنهي الخدمات أو تُنهي العمل. ونذكر هنا عينة من سياســة الاســتخدام المقبول لخدمات بروتوكول الإنترنت لشركة (AT&Ts):

المواد والمحتوى المُهدِد: لا يجوز اســتخدام خدمات بروتوكول الإنترنت في اســتضافة أو نشر أو إعادة نشر أي محتوى أو مادة (أو إنشــاء اســم نطاق أو تشــغيلها من اسم نطاق) تنتهك أو تهدد صحة أو سلامة الآخرين. وأيضاً بالنسبة إلى خدمات بروتوكول الإنترنت التي تســتخدم اســتضافة المواقع المقدمة من شركة (AT&Ts)، تحتفظ شركة (AT&Ts) بحقها في رفض تقديم مثل هذه الخدمات إذا تم تحديد المحتوى على أنه فاحش، أو غير لائق، أو مكروه، أو شرير، أو عنصري، أو افترائي، أو مخادع، أو تشــهيري، أو خائن، أو عنيف بشــكل مفرط أو مُروج لاستخدام العنف، أو ضار للآخرين[٤].

والسياســات تُلــزم المنظمات على معرفة قيمــة المعلومات التي تُنتجها في ســبيل دعم الأصول الفعلية. وأحياناً قد يكون ذلك التحديد وتوثيقه مفيداً في حال التقاضي. على سبيل المثال، تتضمن سياســات معهد ماساتشوستس للتكنولوجيا (MIT) الفقرة التالية من أجل الاحتفاظ بسجل بروتوكول التكوين الديناميكي للمضيف (DHCP).

إن خــادم بروتوكول التكويــن الديناميكي للمضيف (DHCP) مُهيــأ لمعالجة العناوين المتغيرة آلياً حســب الحاجة. ويتم الاحتفاظ بمعلومات الســجل في خادم تحت إدارة نظم المعلومات والتقنية (IS&T) «Information Systems & Technology». كما يتم إرفاق تاريخ الانشــاء بكل ســجل، ويقوم النظــام يومياً بحذف جميع الســجلات التي مضى على إنشائها ٣٠ يوماً[٥].

ومعهد ماساتشوســتس للتكنولوجيا (MIT) ليس المنظمة الوحيدة التي لديها سياسات مكتوبة تتعلق بســجل بروتوكول التكوين الديناميكي للمضيــف (DHCP). فالعديد من

(٤) سياسة الاستخدام المقبول لشركة (AT&Ts)، http://www.corp.att.com/aup/

(٥) سجل استخدام بروتوكول التكوين الديناميكي للمضيف (DHCP) في معهد ماساتشوستس للتكنولوجيا (MIT)، http://ist.mit.edu/about/policies/dhcp-usage-logs

الجامعــات تفعل ذلك لســبب محدد وهو: لجعل المنظمات التــي تراقب انتهاكات قوانين حقــوق النشر تدرك أنه يجب عليها أن تخطر المنظمــة في غضون ٣٠ يوماً (وذلك في حالة معهد ماساتشوستس للتكنولوجيا) من اكتشاف الحادث.

كـما أن السياســات تضمــن الاتســاق في جميع أنحــاء المنظمة، والاتســاق أمر جيد. فالمنظمات الأكاديمية، على ســبيل المثال، يُعرف عنها بأنها لا مركزية. فقد يكون لكل كلية مجموعــة حوســبة خاصة في كل وحدة إداريــة. ومن حيث الدعم الفنــي، هذا النموذج يضمن أن الأفراد الذي يعملون على محطة العمل يستجيبون للشخص نفسه على أنه مالك محطــة العمل، وفي العادة يكــون عميد الكلية، أما من الناحيــة الأمنية فإن هذا النموذج له القدرة على إنشــاء الحلول الحاسمة لمعظم المشــكلات. على سبيل المثال، قد ترى كلية الهندســة المعمارية أن تطبيقات مكافحة الفيروسات هدر للأموال ومن ثم تقرر عدم شراء أي منها. في حين أن كلية الهندســة قد تقوم بتثبيت تطبيقات مكافحة فيروسات منخفضة الجــودة لمجرد أنها أرخص من غيرها. في حين أن كلية الآداب قد تدفع ثمناً باهظاً للحصول على الترخيص اللازم لأنها لا تملك العدد الكافي من أجهزة الحاســب الآلي لتكون قادرة على التفــاوض على صفقــة أفضل. إن وجود سياســة تؤثر في حلول مكافحة الفيروســات على مســتوى الجامعة يؤدي إلى توحيد هذه الوحــدات، وإجبارها للعمل معاً لتحقيق المعايير، والحصول على نماذج أســعار أفضل، وتحقيق العديد من المزايا الأخرى المرتبطة بالاستخدام المستمر في الحرم الجامعي.

لاحظ أن ما ســبق يختلــف عن عبارة «أنظمة تقنية المعلومات المركزية تعمل بشــكل أفضــل». فحتى لو كان الدعم لا مركزيــاً في المنظمة، فإن بعض الجوانب (مثل الأمن) تُعد الخط الأساس. ويمكن تحقيق ذلك عادة من خلال وضع حد أدنى من القواسم المشتركة. على ســبيل المثال، قد يؤثر معيار إدارة حساب ويندوز (Windows Account Management Standard) في كلمات المرور بحيث لا تكون أقصر من ٨ رموز. وهذا لا يمنع أي إدارة من إنشاء سياسة داخلية خاصة بها بحيث لا تقل كلمة المرور عن ١٢ رمزاً.

وأخيراً فإن السبب الجوهري لموظفي تقنية المعلومات لمساندة تطوير السياسات الأمنية هو دعم الإدارة. وإذا تم تطوير السياســات بالطريقة الصحيحة، فإن المدخلات من جميع

الوحــدات المتضررة ومن جميع أصحاب المصلحة يتم أخذها في الحســبان قبل صدور تلك السياســات. وهذا يُحســن إلى حد كبير قبول أي قيود تفرضها السياسات. وبشكل مشابه للقانون، فإن ادعاء الجهل بالسياسات لا يعفي الأفراد من العواقب، وذلك بمجرد إقرار تلك السياســات. على ســبيل المثال، إذا نصت سياسة المنظمة على أن جهاز الحاسب الآلي الذي لا يقوم بتحديث تعريفات مكافحة الفيروســات يومياً يتم ســحبه من الشبكة، وتم سحب جهاز حاســب آلي لأحد المستخدمين من الشــبكة لهذا السبب فإنه لا يحق لهذا المستخدم التقدم بالشكوى.

دورة حياة السياسات:

بشكل مشابه لدورة الاستجابة للحوادث الأمنية فإن السياسات تعمل أيضاً في دورات. وفي الواقع فإن الحوادث الأمنية تكون غالباً القوة الدافعة وراء إنشــاء سياسات جديدة أو إعادة النظر في السياسات القائمة. ففي أواخر التسعينيات، أدى الانتشار الكبير لفيروس (Melissa) وفيروس (ILOVEYOU) إلى وضع السياســات الأمنية المركزية لتنظيم الجامعات اللامركزي، كما أدى إلى تســمية «مســؤول أمن المعلومــات» (Information Security Officers) في الجامعات.

ويمكن تقســيم المستفيدين من السياســات إلى مجموعتين متميزتين. فالمنظمة تكتب السياســات إما للموظفين والعملاء أو أن السياسات تُكتب استجابة لقوانين الدولة والولاية. ومن الناحية المثالية فإن مسؤول الأمن يستخدم السياسات في التعامل مع كلا المجموعتين.

في بعض الأحيان قد تكون هناك حاجة محددة إلى الرسمية في كتابة السياسات. ولقد رأينا مثل هذه السياســات سابقاً والتي تحتاج إلى مترجم بجانبك عند قراءتها حتى تفهم مضمون السياسات. وكقاعدة عامة لا تستخدم اللغة القانونية إلا إذا كان يتوجب عليك القيام بذلك. فالسياسات تحتاج أن تكون مكتوبة بوضوح وبطريقة يسهل فهم مضمونها من قبل الموظفين والعملاء. والسياســات مكتوبة بلغة غير واضحة تستهدف مجموعة الامتثال التنظيمي، ومن ثم فإنها تصبح «سياسة من أجل السياسة» ولا أحد يقرؤها لأن أفكارها غامضة.

ويجب أن تستهدف السياسات قضايا محددة كلما أمكن ذلك. وتحتوي سياسات بعض المنظــمات على الكثــير من الصفحات، وتتوقــع تلك المنظمات أن يقرأ المســتخدم الوثيقة

كاملة ويفهمها. ومن خلال تقسيم السياسات إلى قطاعات مستهدفة يمكن تحقيق الامتثال التنظيمي، ويمكن كذلك للمستخدم العثور على ما يبحث عنه بسهولة. على سبيل المثال، يمكن أن يكون لديك سياسة مخصصة لحماية البيانات، وأخرى تناقش وصول المستخدم، وثالثة تتحدث عن النسخ الاحتياطي للبيانات.

وقد ذكرنا سابقاً أن السياسات تكون غالباً مدفوعة من قبل الأحداث السلبية. وعندما يكون الحدث كبيراً لجلب اهتمام الإدارة، من الشائع أن نرى ردود فعل متسرعة في شكل من أشكال السياسات. وسوف نناقش «تقييم الأثر» (Impact Assessment) في الأجزاء القادمة، لكن من الجيد أن نتأكد من أن السياسات التي تعيق الإنتاجية والاستخدام لم توضع كرد فعل متهور لحدث من الأحداث السلبية. فأثر السياسات يحتاج إلى دراسة وتحليل قبل اعتمادها من المنظمة، وهذا ينطبق بشكل خاص على السياسات الأمنية.

والسياسات الأمنية يجب أن تكون قوية لحماية خصوصية الأصول وتكاملها وجاهزيتها. ونظراً للحاجة إلى الحماية، تُبالغ الكثير من المنظمات في هذا الجانب. ومع ذلك لا يمكن إعاقة الإنتاجية وتعطيل رسالة المنظمة من أجل تحقيق هذا الهدف. ويميل الموظفون إلى الصراحة والانفتاح بمستوى صراحة السياسات، فالموظفون مجموعة ذات موارد كثيرة تحاول تأدية أعمالها وتحقيق أهدافها بأسهل طريقة ممكنة. فإذا رأى الموظف أن نشاطاً أو سلوكاً هو الأفضل لتحقيق هدفه، وأنت لا تسمح له القيام بذلك، فسوف يجد طريقة للالتفاف حول ذلك. وعندما تضع المنظمات سياساتها، عليها التأكد من أن المستخدم قادر على الالتزام بها.

وفيما يلي سنناقش مراحل دورة حياة السياسات التالية:

- كتابة السياسات.
- تقييم الأثر والإصدار.
- المراجعة.

كتابة السياسات:

الآن حان الوقت لوضع القلم على الورقة وبدء الكتابة الفعلية. وقد يكون لدى المنظمة صيغة محددة لكتابة السياسات. وفي حال غياب تلك الصيغة، يُفضل القيام ببحث على الإنترنت عن السياسات المماثلة لمنظمات في الصناعة نفسها، فإذا كنت تعمل في أحد المدارس عليك البحث في المدارس الأخرى والمناطق التعليمية. ومن المفيد أن تبحث في الولاية التي أنت فيها أولاً لأن في الولاية قضايا امتثال تنظيمية قد تضطر لمعالجتها في الموضوع الذي تواجهه. وبعد ذلك انظر في السياسات الأخرى الوطنية والدولية، وهذا يضمن لك تغطية أكبر عدد ممكن من الموضوعات الفرعية.

ونستعرض هنا قالب عام يتضمن الأقسام التي تحتوي عليها معظم السياسات. وعلى الرغم من أن الأسماء قد تختلف قليلاً، على سبيل المثال البعض يُطلق على «المقدمة» «لمحة عامة»، لكن المحتوى يظل كما هو. ومن أجل الحفاظ على تماثل الموضوع في هذا الجزء فإن جميع الأمثلة التي نستعرضها في هذا الجزء ستكون من التعليم العالي.

لمحة عامة:

وهذا هو الجزء الأول من السياسات. وتُخبر اللمحة العامة المستخدم بأسباب تبني المنظمة لمثل هذه السياسة. وفيما يلي نستعرض مثالاً من السياسة الأمنية العامة (Security Policy)[٦] لجامعة أريزونا (University of Arizona):

موارد الجامعة، والمعلومات والتقنية أصبحت ذات أهمية متزايدة لأعضاء هيئة التدريس والموظفين والطلاب وذلك للأهداف الأكاديمية والإدارية. وفي الوقت ذاته، زادت التهديدات الداخلية والخارجية التي تؤثر في خصوصية تلك الموارد وتكاملها وجاهزيتها. الخروقات الأمنية أصبحت منتشرة، وتستمر الجامعات لتكون هدفاً مرغوباً فيه لتلك الهجمات. موارد الجامعة الحرجة، مثل البحوث ورعاية المرضى والمعاملات التجارية والبيانات الشخصية الخاصة للموظف والطالب، يجب أن تكون محمية من الهجمات ومحمية من الاستخدام أو الاطلاع غير الملائم. فالأجهزة يجب أن تكون مُعدة ومصانة ومحدثة بشكل دوري، وذلك لمنع التسلل والأنشطة الضارة الأخرى.

---

(٦) السياسة الأمنية لجامعة أريزونا، http://security.arizona.edu/is100

في الفقرة الأولى أعلاه وضحت الجامعة أنها تهتم ببياناتها، كما أعطت الفقرة الأولى لمحة عن الموضوعات التي سـيتم تغطيتها في هذه السياسـة، أما في الفقرة الثانية فقد وضحت الجامعة الهدف من وراء كتابة هذه السياسة.

الهدف من هذه السياسة هو التأكد من أن جميع الأفراد الموجودين في نطاقها يفهمون مســؤولياتهم اتجاه الحد مــن مخاطر الاختراق ويأخذون التدابير الأمنية المناســبة لحماية مــوارد الجامعــة. إن الوصول إلى موارد الجامعــة امتياز وليس حقاً، مــما يعني أن هناك مسؤوليات على المستخدم. وهذا الوصول يخضع لأعضاء مجلس جامعة أريزونا وسياسات الجامعة ومعاييرها ومبادئها التوجيهية، كما يخضع للقوانين الاتحادية والفيدرالية.

وذكرت هذه الفقرة بعض المبادئ التوجيهية التي ناقشناها سابقاً. فالأمن ليس وظيفة إدارة تقنيــة المعلومات وحدها، بل إن أمن البيانات مســؤولية كل فــرد في الجامعة. كما وضحــت هــذه الفقرة الزاميــة التنفيذ، حيث أشــارت إلى أن الوصول، بمــا في ذلك وصول الطلاب، ليس حقاً بسبب دفع الرسوم الدراسية بل هو امتياز، وإذا أساء المستخدم إلى هذا الامتياز فإن هناك عواقب لذلك.

النطاق:

قســم النطاق يُخبر المستخدم بالأشــخاص والأمور التي تغطيها السياسات. فالسياسات دائماً ترتبط بنطاق معين. وهنا نذكر على ســبيل المثال السياســة الأمنية لمحطات العمل[٧] (Workstation Security Policy) في كلية إيموري (Emory College):

السياســة الأمنية للأجهزة قابلــة للتطبيق على كافة محطات العمــل (ويندوز، ماك أو إس أكــس، لينكس) (بما في ذلك الأجهزة المكتبية والمحمولة والأجهزة الافتراضية) والتي تقع ضمن النطاق الإداري للكلية.

وهذا النطاق واضح المعالم، وفي لمحة واحدة يســتطع المســتخدم قراءته وتحديد ما إذا كان جهازه مشــمولاً بهذه السياســة أم لا. لكن يجب على المنظمات ألا تلجأ إلى التحديد

(٧) السياســة الأمنية لمحطــات العمــل في كليــة إيمــوري، https://wiki.as.emory.edu/display/ecitprocedures/Workstation+Security+Policy

الدقيق للمستهدف من السياسات ما لم يكن هناك حاجة لذلك. وعند ذكر ويندوز، وماك أو إس أكس، ولينكس، مازال الباب مفتوحاً أمام بعض الثغرات. لكن إذا أضفنا عبارة «... وأنظمة التشغيل الأخرى» في نهاية القائمة عندها سنُغلق تلك الثغرات. وفي الوضع الحالي للسياسة فإنها لا تشمل محطة العمل المكتبية القديمة بنظام سولاريس (Solaris) والتي يعمل عليها أحد أعضاء هيئة التدريس.

وفي مثال آخر على نطاق السياسات، نستعرض فيما يلي النطاق المرتبط بسياسة إدارة الحوادث (Incident Management Policy)[٨] في جامعة ولاية كنساس (Kansas State University):

تطبق هذه الإجراءات على جميع موظفي الجامعة، والوحدات، والمنتسبين والمسؤولين عن الاستجابة للحوادث الأمنية التي تشمل موارد تقنية المعلومات أو بيانات الجامعة.

وتُعد سياسة جامعة ولاية كنساس مثال ممتاز لسياسة إدارة الحوادث (Incident Management Policy) بما في ذلك تصنيف البيانات وخطوط المسؤولية الواضحة جداً. والأمن ليس مسؤولية مجموعة أمن تقنية المعلومات، ولكن بدلاً من ذلك يتم تقاسم المسؤولية مع كل مستخدم، ومن ثم فإن هذا النطاق يشمل أساساً جميع الموظفين والمنتسبين للجامعة في كل مرة تكون بيانات الجامعة معنية بالأمر.

التعريفات:

قد نرى قسماً منفصلاً للتعريفات في الأقسام التي تسبق السياسات والتي تُهيء الوضع للسياسة الفعلية. وهذا القسم مفيد خاصة عندما يكون موضوع السياسة غير واضح للمستفيدين، أو إذا كان النطاق في المنظمة يحتاج إلى مزيد من التوضيح.

ومثالاً على ذلك نستعرض تعريف «المعلومات الصحية الإلكترونية المحمية» (Electronic Protected Health Information) أو اختصاراً (ePHI) من جامعة جورجتون (Georgetown University):

(٨) إدارة الحوادث في جامعة ولاية كانساس، http://www.k-state.edu/its/security/procedures/incidentmgt.html

المعلومات الصحية الإلكترونية المحمية: وتشـمل البيانات الحاسوبية القديمة والحالية والمسـتقبلية ذات العلاقـة بالصحة الجسـمية أو العقلية، أو العـلاج والرعاية الصحية، أو دفع تكاليف الرعاية الصحية. وتشـمل أيضاً المعلومات التي يمكن أن تحدد الفرد كالاسم، ورقم الضمان الاجتماعي، والعنوان، وتاريخ الميلاد، والتاريخ الطبي أو رقم السـجل الطبي، وتشـمل كذلك المعلومات المرسـلة أو المحفوظة إلكترونياً، ولكن باسـتثناء بعض سجلات الطلاب وسـجلات التعليـم. والمعلومات الصحية الإلكترونية المحمية لا تشـمل سـجلات الطالب الدراسية، بما في ذلك السجلات الطبية (والمحمية بموجب قانون «الحقوق التعليمية والخصوصية للأسرة» (FERPA))، والسـجلات الطبية للموظفين والتي اسـتلمتها الجامعة بصفتها صاحب العمل، وسجلات تعويضات الموظفين. وعلى الرغم من أن هذه السجلات لا ينطبـق عليها قانون إمكانية نقل التأمين الصحي والمسـاءلة (HIPPA) أو قواعد الأمن والخصوصية، لكن سياسـات الجامعة الأخرى تغطي خصوصيـة وأمن هذه المواد. كما أن هناك أحكاماً خاصة في القانون تتعلق بنشر سجلات العلاج النفسي.

هذا التعريف مهم للغاية لسياسـة قانون التأمين الصحي وإمكانية الحمل والمحاسـبة (HIPAA)[٩] في جامعـة جورجتون لأن «المعلومات الصحية الإلكترونية المحمية» (ePHI) تُعـد المحور الأسـاسي للوائح (HIPAA). وهذا التعريف لا يحـدد فقط ما يُعد جزءاً من (ePHI) بل يحدد أيضاً بعض الأمثلة الواضحة عما لا يُعد جزءاً من (ePHI) مثل سـجلات الطلاب.

ويُعـد مصطلـح «مـوارد المعلومات» مصطلحاً شـائع الاسـتخدام في سياسـات تقنية المعلومـات. لكن ما الذي يُقصد بموارد المعلومات؟ هل تشـمل تلك الموارد الهاتف الذكي للموظف؟ وهل تشمل جهاز الحاسب الآلي المحمول للطالب؟ وهل تشمل جهاز الفاكس التابع للإدارة؟ وهل تشـمل رقم هاتف عضو هيئة التدريس؟ نستعرض فيما يلي تعريف «موارد المعلومات» في كلية ماريست (Marist College)[١٠]:

لأهداف هذه السياسة، يُقصد بموارد المعلومات ما يلي:

(٩) سياسة قانون التأمين الصحي وإمكانية الحمل والمحاسبة (HIPAA) في جامعة جورجتون، http://policies.georgetown.edu/hipaa/sections/security/62953.html

(١٠) سياسة أمن المعلومات في كلية ماريست، http://security.marist.edu/policy.pdf

١. جميع ما تملكه كلية ماريســت من أجهزة حاســوبية، وبرمجيات، وأجهزة التواصل، وأجهــزة شــبكية، وبروتوكولات الاتصالات والشــبكات، وأجهــزة التخزين المرتبطة والوحدات الطرفية.

٢. الأجهــزة الحاســوبية، والبرمجيات، وأجهــزة التواصل، والأجهزة الشــبكية، وأجهزة التخزيــن المرتبطة والوحدات الطرفية التي تتصل بأي مورد من موارد المعلومات في كلية ماريست.

٣. الأجهــزة الحاســوبية، والبرمجيات، وأجهــزة التواصل، والأجهزة الشــبكية، وأجهزة التخزين المرتبطة والوحدات الطرفيــة التي تحفظ أو تنقل معلومات تختص بكلية ماريست.

٤. جميــع البيانات والمعلومات والملكيــة الفكرية التي تُنقل عــبر أي مورد من موارد المعلومات في كلية ماريست أو تُحفظ فيه.

٥. التقاريــر الورقيــة، والمايكروفيلم، وشرائح الصور المصغــرة (المايكروفش)، والكتب، والأفــلام، وأي وســائط تحتوي على معلومــات، أو بيانات، أو ملكيــة فكرية تعود ملكيتها لكلية ماريست.

وهذا تعريف دقيق جداً لموارد المعلومات. وبعد ورود هذا التعريف في السياسة، يجب ألا يكون هناك أي سؤال حول ما يُقصد بموارد المعلومات.

بيان السياسة:

وأخيراً نأتي إلى الجزء الذي يشرح للقارئ السياســة الفعلية التي نريد تأسيســها. وهذا الجزء يذكر جميع المفاهيم التي عُرضت في الأقســام السابقة: الغرض، والمبادئ التوجيهية للمنظمة، وأهداف السياســة، والتعريفات، وصولاً إلى الخاتمة. ويوضح بيان السياسة كيف تتعامل المنظمة مع قضية معينة.

الفقرة التالية جزء من «الإجراءات والمتطلبات اللاسلكية» (Wireless Requirements and Procedures) في جامعة ماساتشوستس في بوسطن (University of Massachusetts)

وهذه الفقرة تناقش نقاط الوصول اللاســلكية (Wireless Access Points)، وهي النقاط التي تربط بين الجهاز المحمول وبقية الشبكة:

نقــاط الوصول اللاســلكية المتصلة بالبنية التحتية للجامعة يجب أن تكون مســجلة في تقنيــة المعلومات، ويجب أن تكون متوافقة مع المعايــير التقنية ومتوافقة مع مصطلحات التسمية المحددة من قبل تقنية المعلومات. وعملية التسجيل تتطلب معلومات عن الوحدة الجامعيــة المعنية وارتباطهــا المحدد، والموقع، والغرض، وكذلك معلومات فنية وتشــغيلية عن نقاط الوصول اللاســلكية. ويمكن إنهاء عملية التســجيل باستخدام النموذج الإلكتروني الموجود عــلى الموقع الإلكتروني لتقنية المعلومات. ويهدف هذا التســجيل لتعريف نقطة الوصول اللاسلكية، بهدف تسهيل الاتصالات بين جميع الأطراف المسؤولة عن دعم الشبكة اللاســلكية والعمليات، وضمان الامتثال لسياســات الجامعة ومعاييرها ومبادئها التوجيهية، وأيضاً ضمان الامتثال للقواعد واللوائح المحلية والتابعة للولاية والدولة.

وهذا هو النوع الشــائع من السياسات. نقاط الوصول اللاسلكية (WAPs) المنتشرة في الحرم الجامعي بلا مبالاة قد تســبب مشــكلات في الجامعة. فإذا لم تتم الإعدادات بشكل صحيح، فإن الفرد الذي يتجول في الحرم الجامعي قد يرتبط بنقاط الوصول اللاسلكية بالخطأ مــما يعرضه لهجمات التحســس (sniffing attack). وكذلك فإن تتبع الاتصال لمســتخدم معين يصبح غير ممكن بســبب الإعداد غير الصحيح لنقاط الوصول اللاســلكية. ويختلف بيان السياسة في طوله تبعاً للموضوع وتبعاً لاختيار المنظمة، فهناك منظمات تختار تجميع القضايا الأمنية المتعددة في سياسة واحدة في حين أن منظمات تختار تقسيمها إلى سياسات متعددة. وكلما كان ممكناً فإن بيان السياســة يضع الخطوط العريضة لمســؤوليات تنفيذ السياسة.

عند اســتلام «منســق الاســتجابة للحــوادث الأمنيــة» (Coordinator of Incident Response) للتقريــر فإنه مســؤول عن تقييم صحة التقريــر، وتحديد ما إذا كان الحادث يتبع لتقنية المعلومات، ومســؤولاً أيضاً عن تصنيف حوادث تقنية المعلومات، والشروع في إجراءات التعامل مع الحادث.

العبـارة أعلاه جزء من سياسـة الاسـتجابة لحـوادث أمن البيانـات (Data Security Incident Response Policy) في جامعـة بـوردو (Purdue University). وهي واحدة من العديد من العبارات التي تحدد مسؤوليات منسق الاستجابة للحوادث الأمنية.

إلزام التنفيذ:

جزء «إلزام التنفيذ» يكون عادة آخر جزء في السياسة. وقد يشير هذا الجزء إلى سياسات أخـرى لتوضيح العقوبات. كما أنـه من النادر أن يحدد هذا الجـزء العقوبة، ويذكر هذا الجزء عادة مجموعة من التدابير الممكنة مثل عبارة «بحد أقصى وشاملة»، وعبارة «التدابير المناسـبة». وهذا القسم يميل إلى استخدام «يمكن» بدلاً من «يجب» والمستخدمة في بقية أجزاء السياسـة. ونسـتعرض فيما يلي مثالاً على قسم «إلزام التنفيذ» من جامعة كارنيجي ميلون (Carnegie Mellon)[11]:

انتهاك هذه السياسة قد يؤدي إلى تعليق أو فقدان المُخالف لامتيازات الاستخدام، وذلك فيما يتعلق ببيانات المنظمة ونظم المعلومات المملوكة للجامعة. وقد يتم تطبيق عقوبات إداريـة إضافية بالحد الأقصى بما في ذلك الفصل من الوظيفة الجامعية أو فسـخ العقد مع المورد. كما قد يتم تطبيق الإصلاحات الجنائية والمدنية العادلة.

قسـم «إلزام التنفيذ» قد يذكر أيضاً بعض الاسـتثناءات لهذه السياسة، أو الوسيلة التي تتيح للمستخدم التقدم للحصول على استثناء للسياسة. السياسة السابقة نفسها من جامعة كارنيجي ميلون (Carnegie Mellon) تضيف ما يلي:

استثناءات هذه السياسة يجب الموافقة عليها من مكتب أمن المعلومات وذلك بتوجيه من «اللجنة التوجيهيـة والتنفيذية للحوسـبة» (Executive Steering Committee on Computing)، وتوثيق ذلك رسمياً. وسيتم مراجعة استثناءات هذه السياسة بشكل دوري للتأكد من ملاءمتها.

ومكتب أمن المعلومات لا يقوم فقط بقبول أو رفض طلبات الحصول على اسـتثناء بل يقـوم أيضـاً بمراجعة تلك الطلبات من وقت لآخر للتأكد من أنها تتناسـب مع التهديدات

(١١) سياسـة أمـن المعلومـات في جامعـة كارنيجـي ميلـون، http://www.cmu.edu/iso/governance/policies/information-security.html

التكنولوجية الحالية ومن ثم لا تُصبح الجامعة في خطر. وتجدر أيضاً ملاحظة أمر مشــترك في السياســات ورد في هذه الفقرة: ســوف يتم مراجعة الاســتثناءات بشكل دوري. أي أن المراجعة ليســت سنوية ولا شهرية بل دورية. وتتم الصياغة بهذا الأسلوب حتى لا يخالف مكتــب أمن المعلومات السياســة التي وضعها بعدم مراجعة الاســتثناءات في جدول زمني محدد. فعملية المراجعة يمكن تأجيلها عند ظهور مسائل أخرى أكثر أهمية.

وعند اعتماد السياسات من قبل المنظمة فإن الامتثال أمر إلزامي. وفيما يلي مثال آخر من السياســة الأمنية لوزارة الزراعة الأمريكية (USDA). وذكرت هذه السياسة ما ذكرناه آنفاً وهو أن كل من يتعامل مع بيانات وزارة الزراعة يجب أن يمتثل للسياسة الأمنية. وفي الفقرة الأخيرة تناقش السياسة موضوع إلزام التنفيذ.

جميع مستخدمي المعلومات ومستخدمي نظم المعلومات الآلية، متضمناً ذلك الموردين الذيــن يعملون لــوزارة الزراعة، مُطالبون بالامتثال لسياســة أمن نظــم المعلومات وكذلك الامتثال للإجراءات والممارسات التي طورت لدعم هذه السياسة. ويخضع أي مورد يتعامل مع بيانات حساســة لــوزارة الزراعة للمتطلبات الأمنية المنصــوص عليها في النظام الإداري (Departmental Regulation).

ويتحمل أي شــخص يشــتبه في سوء اســتخدامه لموارد نظم معلومات وزارة الزراعة أو محاولة إســاءة اســتخدامها مسؤولية الإبلاغ عن هذا النشــاط إلى المسؤولين الإداريين وإلى مدير برنامج أمن نظم المعلومات (ISSPM).

وســيتم رفع انتهاكات المعايير أو الإجراءات أو الممارســات الداعمة لهذه السياســة إلى المســؤولين الإداريين لاتخاذ الإجراء المناســب متضمناً ذلك الإجــراءات التأديبية والتي قد تشمل الفصل من الوظيفة[١٢].

وهذه الفقرة توضح أمراً شــائعاً في السياســات يتعلق بإلزام التنفيذ. فبدلاً من تحديد أن أي شــخص يقوم بأمر مخالف ســيتم فصله مباشرة من المنظمة، فإن السياســة تُخفف مــن ذلك بقول أن الإجراء التأديبي «يصل إلى» الفصل من الوظيفة. وصياغة العبارة بهذه

(١٢) السياســة الأمنية لــوزارة الزراعــة الأمريكيــة، /http://www.ocio.usda.gov/sites/default/files/docs/2012 htm.001-DR3140

الطريقة تســمح للمسؤولين الإداريين تطبيق العقوبات الخاصة بهم دون الحاجة بالضرورة لفصــل الموظف. وفي الواقع فإن هذه السياســة لا تضع حــداً أدنى لإلزام التنفيذ حيث إن العقوبة المُخففة قد تكون كافية وفقاً للنوايا والمقاصد.

ولا نهــدف هنا أن ننتقد هذه السياســة بالتحديد، لكن من المهم الإشــارة إلى أن هذه السياســة تفتقر إلى نقطــة مهمة ومطلوبة من قبل الإرشــادات التوجيهية التابعة لنموذج «أهــداف التحكم للمعلومــات والتكنولوجيــا ذات الصلــة» (Control Objectives for Information and Related Technologies) والــذي يعــرف اختصــاراً بـــ (COBIT). ويوجد طُرق لتطوير هذه السياســية حيث إن أحد البدائل التي من شــأنها أن تجعل هذه السياسة متوافقة مع نموذج (COBIT) هو النص على فصل الجاني من وظيفته، ثم السماح بطلب الاستئناف في حال وجود ظروف خاصة.

تقييم الأثر والتدقيق:

عند الانتهاء من كتابة السياسة فإنه يُنصح بشدة أن يتم مراجعة السياسة من قبل جميع المســتفيدين المتأثرين من تلك السياسة. وخلال هذه المرحلة يتم تعميم مسودة السياسة على المســتفيدين ويُطلب آراؤهم حولها. وأحد الأسئلة التي تُطرح على المستفيدين هو ما إذا كانت السياســة الجديدة أو التغيير في السياســة الحالية يؤثر في الإدارات المستفيدة أم لا. وعلى المنظمة أن تكون مدركة لأثر فشــل تمرير السياســة الجديدة كإدراكها لأثر نجاح تمرير السياسة.

وعند مناقشــة السياســات وتدقيقها فإن موضوع الحوكمــة (Governance) يأتي على الفور، فالحوكمة ترتبط بالتسلســل الهرمي لاتخاذ القرار في المنظمة. وفي مجال السياسات فــإن الحوكمة تعكــس اللجان والمجموعات التي لديها القدرة على رفض السياســة قبل أن تصبح رسمية. وفيما يلي مثال من جامعة ميشغن (University of Michigan)[١٣]:

فيما يلي المســتويات المختلفة لحوكمة المراجعة والتدقيق للسياسات والمعايير والمبادئ التوجيهية (والتي صيغت مبدئياً من قبل مجموعات العمل الخاصة بتطوير سياسات تقنية المعلومات):

(١٣) نموذج تطوير السياسات في جامعة ميشيغن، http://cio.umich.edu/policy/framework.php

المديــر التنفيذي لأمن المعلومات (CISO) /التدقيق الداخلي (IIA): المراجعة المبدئية للسياسات والمعايير والمبادئ التوجيهية.

مجلس التدقيق الداخلي (IIA): المســتوى الأول لحوكمة مراجعة السياســات والمعايير والمبادئ التوجيهية التابعة لتقنية المعلومات.

مديــر المعلومات (CIO): المســتوى الثاني لحوكمة مراجعة السياســات التابعة لتقنية المعلومــات، والموافقة النهائيــة على المبادئ التوجيهية والمعايير قبــل اعتمادها ونشرها في الحرم الجامعي.

مجلس تقنية المعلومات: المســتوى الثالث لحوكمة مراجعة السياســات التابعة لتقنية المعلومات، السياســات الجديدة أو السياسات التي أُجريت عليها تغييرات جوهرية تتطلب موافقة المجلس.

اللجنة التنفيذية لتقنية المعلومات: المستوى الأخير لحوكمة مراجعة السياسات التابعة لتقنية المعلومات، السياســات الموصى باعتمادها الجديدة أو المُعدلة كـ «دليل الممارســات الموحد» (Standard Practice Guide) تتطلب موافقة اللجنة التنفيذية لتقنية المعلومات.

وقــد يكون هناك مســتويات أخرى لموافقة المعنيين قبل أن تصبح السياســة رســمية. وعمومــاً، من أجــل تطبيق السياســة في المنظمة بأكملهــا، لابد أن يتــم تدقيقها من قبل مجموعات أخرى. فأعضاء هيئة التدريس وربما حتى المنظمات الطلابية قد يكون لهم رأي في السياسة. وبعض الجامعات لديها «مجموعات سياسة» محددة ومعدة بحيث يكون لها تمثيل في الحرم الجامعي، وتكون مسؤولة عن مراجعة السياسات والموافقة عليها أو رفضها. وتتعامل جامعات أخرى مع السياســات من خلال مكتب المستشــار العام. وفيما يلي مثال من جامعة كورنيل (Cornell University)[١٤]:

بعد موافقة الســلطة التنفيذية المســؤولة، يقوم مكتب السياسات في الجامعة (UPO) بتوزيع وثيقة مسودة السياسة على أعضاء الفريق الاستشاري (Policy Advisory Group) قبل اجتماع أعضاء الفريق. وتقوم الســلطة التنفيذية المسؤولة أو المكتب المسؤول بعرض

(١٤) صياغــة وإصــدار سياســات جامعــة كورنيــل، http://www.dfa.cornell.edu/cms/treasurer/policyoffice/policies/volumes/governance/upload/vol4_1.pdf

مســودة السياســة في الاجتماع حيث يتم مراجعــة مدى واقعية ووضــوح الوثيقة. وبعد اجتماع أعضاء الفريق الاستشــاري، يقوم مكتب السياســات في الجامعة والمكتب المسؤول بمراجعة السياســة وإجراء التغييرات المقبولة والمقترحة من قبل أعضاء الفريق الاستشاري. وبعد ذلك يقترح أعضاء الفريق الاستشاري أن تقوم مجموعة مراجعة السياسات التنفيذية (EPRG) بالموافقة على الوثيقة التي تم مراجعتها.

وبعد موافقة الســلطة التنفيذية المسؤولة، يقوم مكتب السياسات في الجامعة (UPO) بتوزيع مســودة السياســة النهائية على مجموعة مراجعة السياســات التنفيذية (EPRG) قبل اجتماع أعضاء المجموعة. وتقوم الســلطة التنفيذية المسؤولة بعرض مسودة السياسة النهائيــة في الاجتماع حيث يتدارس أعضاء مجموعة مراجعة السياســات التنفيذية الموافقة النهائية على السياســة، ولاسيما مبادئ تلك السياسة. ويقوم مكتب السياسات في الجامعة والمكتب المســؤول بإجراء التغييرات وفقاً لتوجيهات مجموعة مراجعة السياسات التنفيذية (EPRG).

وبمجرد موافقة مجموعة مراجعة السياســات التنفيذية (EPRG) والســلطة التنفيذية المســؤولة على الوثيقة، يقوم مكتب السياســات في الجامعة (UPO) بكتابة تاريخ الموافقة النهائيــة وتوثيــق هذا التاريخ بأنه التاريخ الذي تم فيه إصــدار الوثيقة، كما يقوم المكتب بنشر السياسة إلى المجتمع الجامعي من خلال إعلان رسمي.

ويقوم مكتب السياســات في الجامعة (UPO) بمعالجة عملية إصدار السياســات. أما أعضاء الفريق الاستشــاري فهم مجموعة متعددة الوظائف مسؤولة عن عمليات الموافقة. وفي جامعة كورنيل يجتمع أعضاء الفريق الاستشــاري من وقت لآخر لاتخاذ القرارات التي تتعلق بالسياســة. وفي الجامعات الأخرى يمكن أن تتم عملية التدقيق عبر البريد الإلكتروني مع تحديد موعد نهائي للإنجاز.

وكما ترى قد يســتمر الحديث لعدة أســابيع قبل الوصول إلى مرحلة إصدار السياســة وجعلها إلزامية التنفيذ. وهذا أحد الأسباب التي من أجلها يجب أن تترك التفاصيل التقنية خارج السياسات قدر الإمكان. وبإضافة إشارة إلى المعيار الموجود في السياسة، وجعل إدارة تقنية المعلومات المســؤولة عن المعيار، يمكن تعديل الأمور التقنية، ومن أمثلة ذلك: الحد

الأدنى لطول كلمات المرور، وأنظمة التشغيل المعتمدة، وغيرها من عناصر تقنية المعلومات المتغيرة والتي يمكن تعديلها بسهولة أكبر من خلال المراجعة الداخلية.

وبينما تبدو هذه المراجعة الواسعة بأنها بيروقراطية غير ضرورية، لكنها في الواقع تمنع المنظمة من تطوير سياسات صعبة التنفيذ، كما تمنع تطوير السياسات التي لها عواقب غير مقصودة بين المستفيدين. وقبل الحاجة إلى تنقيح السياسات بسبب مواجهة مقاومة من المستفيدين، من المهم النظر في جميع المشكلات المحتملة في السياسات قبل رفعها إلى الإدارة العليا لطلب موافقتها، وذلك حتى لا تؤثر في مصداقيتك لدى إدارة المنظمة.

مراجعة السياسة:

عند إنشاء السياسة أو المعيار ونشرها، متى ينبغي إعادة النظر فيها؟ هناك بعض المؤشرات التي ينبغي أخذها في الحسبان لكن أكثرها شيوعاً هو المراجعة الدورية للسياسات. وعادة ما تكون الجامعات معتمدة من قبل منظمات أكاديمية خارجية. ففي فلوريدا، منظمة الاعتماد هي «الرابطة الجنوبية للكليات والمدارس» (Southern Association of Colleges and Schools) أو اختصاراً (SACS). وفي كل خمس سنوات تقوم رابطة (SACS) بإرسال فريق من المحققين الأكاديميين إلى الجامعة، وذلك للنظر في الدرجات العلمية التي تقدمها الجامعة والسياسات والإجراءات العامة فيها. وأحد الأمور المحددة التي تنظر فيها رابطة (SACS) هو ما إذا كانت الجامعة تراجع السياسات بشكل دوري متضمناً ذلك سياسات تقنية المعلومات. فإذا كان عمر السياسة عشر سنوات، فهل تم مراجعتها مؤخراً؟ وهل تلبي هذه السياسة الاحتياجات الحالية للمنظمة؟ وإذا لم يكن الحال كذلك، فهل يعكس ذلك إهمال منظم من جانب تقنية المعلومات؟ والقاعدة العامة هو أن يكون هناك مراجعة داخلية لجميع السياسات والمعايير والمبادئ التوجيهية مرة واحدة على الأقل في كل عام. وعادة ما يكون الأشخاص في تقنية المعلومات والمسؤولون عن إدارة النظام، هم المسؤولين إلى حد ما عن كتابة السياسات. وفترة المراجعة السنوية هي الوقت الذي يتم فيه النظر في جميع المؤشرات لتحديد ما إذا كانت السياسة تحتاج لمراجعة.

وأحد الأمور التي من شأنها أن تُسرع في مراجعة السياسات والمعايير هو ظهور التغيرات التكنولوجية. ومن الناحية المثالية، تُكتب السياسات بحيث يمكن التعامل مع

التكنولوجيـا الحديثة من خـلال المعايير بدلاً من الاضطـرار إلى اللجوء إلى عملية إصدار السياسات كاملة.

كما أن المشروعات الجديدة التي تنشر تطبيقات جديدة أو مُحدثة قد تتطلب مراجعة. على سبيل المثال، تغيير بوابة الموظفين إلى تطبيق جديد يمكن أن يكون تجربة كبيرة تحتاج في الوقت ذاته إلى تغيير في السياسات والمعايير والمبادئ التوجيهية.

أمـا التغييرات في الامتثـال التنظيمي قد تتطلـب إعادة تقييم للحوكمة. على سـبيل المثال، يُجبر قانـون «فرصة التعليم العـالي» (Higher Education Opportunity Act) لعـام ٢٠٠٨، والذي يعرف اختصاراً (HEOA)، الجامعـات لاتخاذ موقف أكثر صرامة ضد المشـاركة غير الشرعية للمـواد المحمية الحقوق مثـل الأفلام أو الموسـيقا. ووفقاً لمنظمة (EDUCAUSE)[(١٥)]، فـإن العديد من أقسـام قانون (HEOA) تعالـج تبادل الملفات غير المصرح به على شبكات الجامعات مما أدى إلى فرض ثلاثة شروط عامة على جميع الكليات والجامعات الأمريكية:

- كشـف سـنوي يوضح للطلاب قانون حقوق النشر وكذلك سياسات الحرم الجامعي المتعلقة بانتهاك حقوق النشر.
- خطـة لـ «القضاء الفعال على التوزيـع غير المصرح به للمواد المحمية الحقوق» من قبل مسـتخدمي الشـبكة، بما في ذلك «اسـتخدام واحد أو أكثر من أسـاليب المنع التكنولوجية».
- خطة لـ «توفير بدائل لعمليات التحميل غير المشروعة».

ووفقـاً لهذا القانـون، كان مطلوباً من الجامعات أن تبذل جهداً للامتثال بحلول شـهر أغسـطس من عـام ٢٠٠٨، على الرغم من أنه لم يتم الالزام بتنفيـذ القانون إلا بحلول عام ٢٠١٠. وعـدم الامتثال قد يؤدي إلى خسـائر مالية كبيرة عـلى الجامعة، وذلك من جانب المساعدات المالية التي تقدمها الحكومية. وقد أدى التغيير في الامتثال إلى تغيير في العمليات، والذي يجب أن ينعكس على شكل تغييرات في السياسات الحالية.

(15) HEOA of 2008, EDUCAUSE, http://www.educause.edu/library/higher-education-opportunity-act-heoa

الامتثال:

قبل أن نناقش بعض الأمثلة وبعض القضايا الرئيسية المتعلقة بالسياسات، سنناقش موضوع عادة ما يُساء فهمه وهو موضوع الامتثال. والأهم من ذلك أن نفهم الفرق بين البيئة الآمنة والبيئة المُمتثلة.

الامتثال، والذي يشار إليه أحياناً بالامتثال التنظيمي، يتضمن اتباع المواصفات التي وضعتها السياسات والمتطلبات القانونية. وغالباً ما تنشأ السياسات من: (أ) معايير الصناعة المنطلقة من الامتثال التنظيمي، أو (ب) الأحداث ذات الآثار السلبية على المنظمة. وهذه المواصفات القانونية غالباً ما تكون غامضة ومُحيرة خصوصاً في حال الامتثال المفروض من قبل قانون الولاية وقانون الدولة. على سبيل المثال، تسرب أرقام الضمان الاجتماعي (Social Security Numbers) في السنوات الماضية أدى إلى تأسيس العديد من قوانين الولاية التي تفرض حماية أرقام الضمان الاجتماعي، لكن تلك القوانين لم تعالج الأسباب الذي يتعين من أجلها قيام المنظمات بجمع أرقام الضمان الاجتماعي.

لكن من المهم للمحلل الأمني أن يفهم الفرق بين الأمن والامتثال. دعنا نفترض أنك، على سبيل المثال، تحتفظ بخادم آمن للغاية ويحفظ هذا الخادم «بيانات مقيدة» تابعة للمنظمة التي تعمل فيها. وفي هذا الخادم الافتراضي تحتفظ المنظمة بآلاف من معلومات بطاقات الائتمان الخاصة بالعملاء. كما أنك قمت في مثالنا هذا بإعداد ٢٠ نوعاً من الضوابط للحفاظ على أمن النظام، ومن تلك الضوابط: حساب واحد لا يعرفه إلا أنت، والمصادقة المتعددة العوامل، والجُدر النارية، وغيرها. وبغض النظر عما فعلت لحماية البيانات، فإنه إذا لم يتم تشفير بيانات بطاقات الائتمان، فإن النظام قد لا يفي بمتطلبات الامتثال وفقاً لسياسة «صناعة بطاقات الدفع» (Payment Card Industry).

وهذا لا يعني أن الامتثال ليس مهماً حيث تتأكد إدارة التدقيق والامتثال الداخلية (Internal Audit and Compliance) من التزام المسؤولين وبقية الموظفين بالقوانين والسياسات التي تدير المنظمة، وذلك حتى لا تصبح المنظمة في خطر لا مبرر له. وفي مجال تقنية المعلومات، فإن غياب إدارة التدقيق والامتثال الداخلية، التي تشترك مع تقنية المعلومات في بعض المشاريع، يعني أن مسؤولية التزام جميع المصادر الموضحة في الشكل (١٣-٢) ترجع إلى إدارة تقنية المعلومات. وإذا كان سياق الامتثال غير موجود فإن إدارة

الأمــن وفرق العمليات ســتقوم بما تعتقد أنه صحيح ولكــن يمكن أن يكون ذلك في حقيقة الأمر إضاعة للجهد بسبب عدم تحقيق النتائج المرجوة.

إن الامتثال جانب أســاسي لأي مشروع، ولــذا ينبغي الاهتمام بالامتثال مبكراً في مراحل التخطيــط للمشروع. فتصميم المــشروع والامتثال التنظيمي في الاعتبار، أســهل بكثير من التعديل والتكييف وفقاً للمتطلبات بعد الانتهاء من المشروع.

الشكل (١٣-٢): الامتثال



وكل ولايــة لديها مجموعة مــن متطلبات الامتثال التنظيميــة. وبعض تلك المتطلبات موجهــة مباشرة نحو مــوارد تقنية المعلومات مثــل قانون الإشــعار بالاختراقات (Breach Notification Law) التابــع لولاية كاليفورنيا. ووفقاً لموقــع (datagovernance.com)، فإن قانون معلومــات الاختراقات الأمنية التابع لولاية كاليفورنيــا (California Security Breach Information Act) رقــم (SB 1386) هــو قانون في ولاية كاليفورنيا يتطلب من الــشركات التي تجمع معلومات شــخصية أن تقوم بإشــعار كل شــخص موجود في قاعدة بياناتهــم في حال حدوث اختراق أمنــي يتضمن معلوماتهم الشــخصية مثل أرقام الضمان الاجتماعي، وأرقام الحســابات، أرقام البطاقات الائتمانية وبطاقات الصرف الآلي، أو الرموز الأمنية أو كلمات المرور المرتبطة بالوصول لحساباتهم المالية.

والقوانــين الأخرى تؤثر بشــكل غير مبــاشر في تقنية المعلومات مثــل قوانين الاحتفاظ بالســجلات (Record Retention) في ولاية فلوريدا. وتُعد هذه القوانين مجموعة معقدة

مــن اللوائح تحتوي على جــداول الاحتفاظ والتي تحدد ســجلات المنظمة، كما تضع الحد الأدنى للفــترات الزمنية اللازمة للاحتفاظ بالســجلات اســتناداً إلى القيمــة الإدارية والمالية والقانونية والتاريخية للسجلات[١٦].

وبالإضافــة إلى متطلبات الولاية، هناك أيضاً متطلبــات الامتثال الفيدرالية التي وُضعت مــن قبل العديد من القوانين واللوائــح المختلفة اعتماداً على نوع الصناعة أو نوع البيانات التــي تعالجها المنظمة. وبشــكل مشــابه للوائح الولاية، فإن بعــض المتطلبات الفيدرالية موجه بشــكل مباشر لموارد تقنية المعلومات. وبعض تلك المتطلبات يؤثر بشكل غير مباشر في تقنية المعلومات. ونســتعرض فيما يلي بعضاً من اللوائح الفيدرالية الأكثر شــهرة والأكثر تعقيداً، وكلٌّ من هذه اللوائح يســتغرق ما لا يقل عن أســبوع كامل لدراســتها، لذا سوف نستعرض هذه اللوائح بإيجاز.

قانون التأمين الصحي وإمكانية الحمل والمحاسبة (HIPAA):

لائحة الخصوصية التابعة لقانون (HIPAA) تُقدم حماية فيدرالية للمعلومات الصحية الشخصية المحفوظة في المنظمات المشمولة، كما تُعطي تلك اللائحة المرضى تنظيماً للحقوق المتعلقة بتلك المعلومات. وفي الوقت نفســه فإن لائحة الخصوصية متوازنة بحيث تســمح بالكشــف عن المعلومات الصحية الشــخصية اللازمة للعناية بالمــرضى أو اللازمة للمقاصد الهامة الأخرى.

كما تحدد لائحة الخصوصية سلســلة من الضمانات الإدارية والمادية والفنية لاستخدام المنظمات المشمولة لضمان خصوصية المعلومات الصحية الإلكترونية وتكاملها وجاهزيتها[١٧] .

قانون التجديد المالي (GLB) (Financial Modernization Act):

ويتطلــب هذا القانون من «المنظمات المالية» حمايــة خصوصية عملائها متضمناً ذلك المعلومات الشــخصية وغير العامة للعملاء. وبمــا أن الجامعات تتعامل أيضاً مع مجموعة متنوعــة من الســجلات المالية تختص بالطــلاب وأولياء أمورهم، فإنها مســؤولة عن أمان

(١٦) جدولة الاحتفاظ بالسجلات وترتيبها، http://dlis.dos.state.fl.us/recordsmgmt/scheduling.cfm

(١٧) فهم خصوصية المعلومات الصحية، http://www.hhs.gov/ocr/privacy/hipaa/understanding/index.html

السجلات الشخصية لطلابها. ومن بين المنظمات التي تخضع لهذا القانون منظمات الإقراض والرهن غير البنكية، وسماسرة القروض، وبعض المستشارين الماليين ومستشاري الاستثمار، ومُعدي الضرائب، ومُقدمي خدمات التسوية العقارية، ومُحصلي الديون. وفي الوقت ذاته فإن لوائح هذا القانون تنطبق فقط على المنظمات التي «تعمل بشكل كبير» في الأنشطة المالية.

ويتكون هذا القانون من نوعين من القواعد: قاعدة الحماية (Safeguards Rule)، وقاعدة الخصوصية (Privacy Rule). ووفقاً للموقع الإلكتروني لهذا القانون، فإن قاعدة الحماية تتطلب من المنظمات تطوير خطة مكتوبة لأمن المعلومات تصف فيها برنامج لحماية معلومات العملاء. ويجب أن تكون الخطة متناسبة مع حجم المنظمة والتعقيد الموجود فيها، وطبيعة ونطاق أنشطتها، وأهمية معلومات العملاء التي تعالجها. وكجزء من هذه الخطة يجب على المنظمة ما يلي:

- تعيين موظف واحد أو أكثر لتنسيق برنامج أمن المعلومات لديها.
- تحديد المخاطر المرتبطة بمعلومات العملاء وتقييمها في كل مرحلة من مراحل عمليات المنظمة، وتقييم فاعلية الحماية الحالية لضبط تلك المخاطر.
- تصميم وتطبيق برنامج الحماية، ومراقبة واختبار ذلك البرنامج بشكل منتظم.
- اختيار مزود الخدمات الذي يستطيع الحفاظ على الحماية المناسبة، والتأكد من أن العقد يتطلب منه الحفاظ على تلك الحماية، والإشراف على تعامله مع العملاء.
- تقييم وضبط البرنامج بناءً على الظروف المحيطة متضمناً ذلك تغير مجال أعمال المنظمة أو عملياتها، أو تغير نتائج الاختبارات والمراقبة الأمنية.

قانون «الحقوق التعليمية والخصوصية للأسرة» (FERPA):

قانون «الحقوق التعليمية والخصوصية للأسرة» أو اختصاراً (FERPA) رقم (U.S.C, 20 1232g, 34 CFR) هو قانون فيدرالي يحمي خصوصية السجلات التعليمية للطالب. وينطبق هذا القانون على جميع المدارس التي تتلقى دعم مالي في إطار البرنامج المطبق في وزارة التعليم الأمريكية (US Department of Education).

وقد تكشــف المدارس، دون وجود موافقة خطية، عن دليل من المعلومات يحتوي على اســم الطالب، وعنوانــه، ورقم هاتفه، وتاريخ ومكان الميلاد، والأوســمة والجوائز، وتواريخ الحضــور. لكــن يجب على المــدارس أن تُخبر أوليــاء الأمور والطلاب المؤهلــين عن دليل المعلومــات، وإعطائهم الوقت الكافي لطلب ألا تقوم المدارس بالكشــف عن معلوماتهم في دليــل المعلومات في حــال رغبتهم ذلك. كما يجب على المدارس ســنوياً إبلاغ أولياء الأمور والطــلاب المؤهلين بحقوقهم بموجب قانون (FERPA). أما آلية الإبلاغ (رســالة خاصة، أو إدراجها في نشرة جمعية أولياء الأمور والمدرســين (PTA)، أو في كتيب دليل الطالب، أو في مقال صحفي) فمتروك أمرها لاختيار كل مدرسة[18].

قانون ساربينز أوكسلي (Sarbanes-Oxley Act):

قــدم قانــون ســاربينز أوكســلي (Sarbanes-Oxley Act) أو اختصــاراً (SOX) لعام ٢٠٠٢ تغييرات كبيرة في الممارســات المالية وتنظيــم إدارة الشركات. وصدر هذا القانون في أعقــاب العديد من فضائح الشركات، وهو قانون معقد من التشريعات التي تتطلب إجراء تغيــيرات كــبرى في الشركات من أجل تحقيق الامتثال في منظماتهــم. ويُحمّل هذا القانون كبار المسؤولين التنفيذين المسؤولية الشخصية عن دقة وحداثة المعلومات المالية للمنظمة، وذلــك تحت تهديــد الملاحقة الجنائية. ولذلك أصبح الامتثال لهــذا القانون أولوية قصوى للشركات المتداولة ذات الملكية العمومية.

ووفقــاً للقانــون الفيدرالي فإن إدارة تقنية المعلومات تلعب دوراً رئيســياً في تأمين دقة وموثوقيــة بيانات المنظمات. ومع تطبيق قانون (SOX) أصبحت ضوابط تقنية المعلومات أكثر انتشاراً. ونذكر هنا بعضاً من عمليات تقنية المعلومات التي من المرجح أن يتم فحصها عند التحقق من الامتثال:

- إدارة الأمن.
- النسخ الاحتياطي للبيانات.
- التحكم في التغيير.
- التحكم في الوصول.

(١٨) الموقع الإلكتروني لوزارة التعليم الأمريكية، http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html

قوانين الرقابة على التصدير:

يُعــد موضوع قوانين الرقابة على التصدير موضوعاً ســاخناً للجامعات البحثية في جميع أنحاء البلاد. فالقوانين تمنع التصدير غير المرخص لمواد أو معلومات معينة، وذلك لأســباب ترجــع للأمن الوطني وحماية التجارة الوطنية. وعادة ما يُثار موضوع الرقابة على التصدير لأحد الأسباب التالية:

- إذا كانــت طبيعة التصدير لها تطبيقات عســكرية فعلية أو محتملة أو ذات علاقة بقضايا الحماية الاقتصادية.
- إذا كان هناك مخاوف للحكومة بشأن المرسل إليه سواء كان دولة أم منظمة أو فرداً.
- إذا كان هناك مخاوف للحكومة بشــأن الاســتخدام النهائي المُعلن أو المشتبه به، أو مخاوف الحكومة بشأن المستخدم النهائي في عملية التصدير[١٩].

وتخضع الجامعات البحثية لقوانين التصدير بما في ذلك «لوائح التداول الدولي للأسلحة» (International Traffic in Arms Regulations) والمعروفــة اختصــاراً (lTAR). وقــد يتــم تطبيق هذه القوانين أيضاً في الحرم الجامعي عــلى التصدير المؤقت للأجهزة المملوكة للجامعة متضمناً ذلك أجهزة الحاســب الآلي المحمولة التي تحتوي على برمجيات أو بيانات فنية مُراقبة، وكذلك على شحن المواد البحثية للمتعاونين الأجانب.

موضوعات رئيسية ذات علاقة بالسياسات:

وفيــما يلي ملخص سريع لبعض الموضوعات الرئيســية التي يتوجب على أي منظمة أن تكون مستعدة للتعامل معها سواء على مستوى السياسات أو على مستوى المعايير.

الاستخدام المقبول: سياسة الاستخدام المقبول هي واحدة من أهم السياسات الرئيسية في المنظمة. وتوضح هذه السياســة إرشادات للمستخدمين والعملاء بما هو مناسب للقيام به باســتخدام موارد تقنية المعلومات وما هو غير مناســب. وتعريف النطاق مهم في هذه السياســة، وذلك حتى يعرف المســتخدم ما الذي يندرج تحت هذه السياســة. وسياســة

(19) UC Berkeley, Export Controls, http://www.spo.berkeley.edu/policy/exportcontrol.html

الاســتخدام المقبول للعميل قد تختلف عن سياسة الاستخدام المقبول للموظف. وعادة ما تكون هذين السياستين متشابهة في البيئة الجامعية. وإذا كان هناك أي استثناءات لتغطية هذه السياســية يجب أن يتم ذكرها. على ســبيل المثال، سياسة الاستخدام المقبول في كلية الطب قد تكون أكثر صرامة نتيجة لضرورة للامتثال لقانون (HIPAA).

تصنيف المعلومات: وتقوم هذه السياسة بتحديد تعريفات أهمية الأصول وحساسيتها، والأمثلــة مهمة لتوضيح الغرض من التصنيف. كما تُعد تعريفات ملكية البيانات والوصاية عليها جزءاً مهماً من هذه السياسة.

الوصول للشــبكة: وهذه السياسة تحدد أنواع المستخدمين الذين يسمح لهم بالوصول إلى موارد الشــبكة والموارد الحاسوبية. الطلاب في صالات الإقامة قد لا يكون لديهم وصول للشبكات الفرعية لمركز البيانات. وقد يضطر أعضاء هيئة التدريس الزائرين للمرور بعملية خاصة من أجل الحصول على امتيازات الشــبكة. وقد يســتطيع الزوار الوصول إلى الشبكة اللاسلكية الخاصة بالضيوف إذا استخدموا أرقام هواتفهم الجوالة في عملية التسجيل.

الوصول عن بعد: وتحدد هذه السياســة الوســائل المقبولة التي يُســمح للموظف من خلالها بالوصول إلى الموارد من خارج شــبكة المنظمة. وقد تشــمل هذه السياســة شروط الوصول للبيانات من خلال الهواتف الذكية والأجهزة الشــخصية الأخرى. وهذه السياســة تحدد أيضاً ما إذا كان اســتخدام «بروتوكول ســطح المكتب عن بعد» (remote desktop) خياراً مقبولاً أم على الموظف استخدام «الشبكة الخاصة الافتراضية» (VPN).

التشــفير: مــا نوع البيانات التي تحتاج إلى تشــفير؟ ومتى يحتاج خادم الشــبكة إلى استخدام طبقة المنافذ الآمنة (SSL)؟ وهل تحتاج بيئة الاختبار والتطوير إلى تشفير؟ وهل بالإمكان أن يتم التوقيع ذاتياً على التصديقات؟ وهل من المقبول أن يتم إرسال المعلومات المقيدة عبر البريد الإلكتروني وهي غير مشفرة؟

التخطيط للطوارئ: وتحدد هذه السياسة خطط التعافي من الكوارث. وينبغي أن تضع السياســة خطاً واضحــاً للقيادة في حال وقوع كارثة محلية او كارثــة عامة، وتوضح الخطة أيضاً التسلسل الوظيفي وبدائل ذلك التسلسل في حال عدم إمكانية الوصول إلى شخص ما. كما تحدد الخطة مديراً تنفيذياً باعتباره الشــخص المناسب ليكون مسؤولاً عن التصريحات

المرتبطة بالكارثة. وتشـير السياسـة أيضاً إلى المعايير والإجراءات الأخرى المرتبطة بتفاصيل حول ما يجب فعله مع كل نظام في حال وقوع الكارثة.

الاسـتجابة للحوادث الأمنية: وتصف هذه السياسـة الإجراءات العامة في حال وقوع حوادث أمنية ذات تأثير سـلبي على المنظمة. وتحدد هذه السياسة الشخص الذي يفترض أن يرأس فريق الاسـتجابة للحوادث الأمنية، وتحدد أيضاً الشـخص المسؤول عن الاتصالات الداخلية والخارجية. كما تحدد السياسة الوقت المناسب لتصعيد الحادث، وكيفية التعامل مـع ذلك التصعيد. كما تُقدم هذه السياسـة لرئيس (فريق الاسـتجابة للحوادث الأمنية) المدى المناسب لاتخاذ قرارات سريعة من جانب واحد من أجل حماية أصول المنظمة.

المصادقـة والتصريح: ما الطرق المقبولة للمصادقة؟ وما الأدوار التي يمكن أن يأخذها المسـتخدم الفردي؟ ومتى يتم إلغاء حساب المستخدم الذي انتهى عقده الوظيفي؟ وهل يُسـمح للإدارة بطلب تمديد هذه الفترة الزمنية؟ ومن له الحق في الحصول على حسـاب على النظام؟

نموذج حالة - شركة (HB Gary):

شركـة (HB Gary) هـي شركة أمن معلومات، ولديها شركة فرعية باسـم (HB Gary Federal). وكـما يوحي اسـم هذه الشركـة الفرعية، فإنها تهدف إلى جـذب أعمال أمن المعلومـات من مختلف الـوكالات الفيدراليـة في الولايات المتحدة مثـل وكالة المخابرات المركزية (CIA)، ومكتب التحقيقات الفيدرالي (FBI)، وغيرها. وبسـبب ضعف برمجيات الشركـة وضعف تنفيذها لسياسـات كلمات المرور، فقد تم سرقة معظم حسـابات البريد الإلكـتروني للشركـة من قبل قراصنة حاسـب متعاونـين مع مجموعـة (Anonymous)، ومجموعة (Lulzsec) وكان ذلك تقريباً في شـهر فبراير من عام ٢٠١١. وأدى انتشـار هذا الحادث وشـيوعه إلى جعل هذه الشركة أضحوكة لأنها شركة أمنية، وفي الوقت ذاته تسعى للحصول على أعمال أمن المعلومات من منظمات تتطلب أعلى مسـتويات الأمن في العالم. وفي الثاني من شهر مايو من عام ٢٠١٢ اتهم المدعي الاتحادي خمسة أشخاص بهذا الحادث كما اتهمهم بجرائم أخرى مرتبطة بها.

وقــد شرح مقال في الموقــع الإلكتروني (Ars Technica) هــذا الهجوم بالتفصيل حيث قامت شركة (HB Gary) بتطوير نظام مخصص لإدارة المحتوى (content-management system) بمســاعدة شركــة أخرى. والثغــرات الموجودة في نظــام إدارة المحتوى جعل من البرمجيــات عرضة لهجمات حقن تعليمات الاســتعلام البنيويــة (SQL injection). ومن خلال استغلال هذه الثغرة، قام المهاجمون بتحميل كامل معلومات المستخدمين من الموقع. وعلى الرغم من أن كلمات السر كانت مشــفرة، إلا أن اثنين من كبار المسؤولين التنفيذين - وهــما الرئيس التنفيذي للشركة (Aaron Barr)، ومدير العمليات (Ted Vera) - لم يلتزما بالتوصيــات العامة لكلمات المرور من جهتين: (١) أنهما اســتخدما كلمات مرور بســيطة، (٢) أنهما اســتخدما كلمة المرور نفســها ليس لنظام إدارة المحتوى فحسب بل أيضاً للبريد الإلكــتروني، وتويتر(Twitter)، وينكدإن (LinkedIn). وهذه المعلومات عن اثنين من كبار التنفيذين والذين لديهم صلاحيات عالية، بالإضافة إلى شيء من الهندسة الاجتماعية الذكية، قد ســمح للمهاجمين بتحميل جميع الرســائل الإلكتروني للشركة، كما ســمح لهم بتشــويه الموقع الإلكتروني للشركة.

ومــن المُمتع قراءة لائحــة الاتهام، وقراءة المقــال الموجود في الموقــع الإلكتروني (Ars Technica) بهــذا الخصــوص، وكذلــك قراءة مقــال موقع ويكيبيديا بخصــوص مجموعة (Lulzsec)[٢٠].

المراجع:

http://arstechnica.com/tech-policy/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack/

http://www.wired.com/images_blogs/threatlevel/2012/03/Ackroydet-al.-Indictment.pdf

http://en.wikipedia.org/wiki/LulzSec

(20) Stephen Colbert had his take on the incident, «Corporate hacker tries to take down Wikileaks,» http://www.colbertnation.com/the-colbert-report-videos/375428/february-24-2011/corporate-hacker-tries-to-take-down-wikileaks (accessed 07/23/2013). Warning: NSFW (not safe for work)

الملخص:

في هذا الفصل ميزنا بين الامتثال والأمن. فبينما يشير الامتثال إلى اتباع إجراءات محددة فإن الأمن يشــير إلى التقليل من الضرر. كما ميزنا في هذا الفصل بين السياســات والمعايير والإجراءات، وهي ثلاثة أشــكال رئيســية للوثائق الرســمية التي توجه أمــن المعلومات في المنظمة. ونظراً للأهمية النســبية للسياسات، ناقشنا في هذا الفصل العملية الشاملة لوضع السياســات التي يؤمل أن تحقق أهدافها. كما ذكرنا في هذا الفصل الحد الأدنى لسياســات أمن المعلومات والتي نعتقد أن على كل منظمة إعدادها.

المرجع:

SANS Policy Templates, http://www.sans.org/security-resources/policies/

أسئلة مراجعة للفصل:

١. ما سياسات أمن المعلومات؟

٢. ما الهدف من سياسات أمن المعلومات؟

٣. ما المعيار؟

٤. كيف تختلف المعايير عن السياسات؟ وما أوجه الشبه بينهما؟

٥. ما المبادئ التوجيهية؟

٦. كيف تختلف المبادئ التوجيهية عن المعايير والسياسات؟ وما أوجه الشبه بينها؟

٧. ما دورة حياة السياسات؟ ولماذا تمر مراحل تطوير السياسات في دورة؟

٨. ما الأجزاء التقليدية لسياسة أمن المعلومات؟

٩. ما الذي يتضمنه عادة قسم اللمحة العامة في سياسة أمن المعلومات؟

١٠. ما الذي يتضمنه عادة قسم النطاق في سياسة أمن المعلومات؟

١١. ما الذي يتضمنه عادة قسم التعريفات في سياسة أمن المعلومات؟

١٢. ما الذي يتضمنه عادة قسم بيان السياسة في سياسة أمن المعلومات؟

١٣. ما الذي يتضمنه عادة قسم إلزام التنفيذ في سياسة أمن المعلومات؟

١٤. مــا تقييم الأثر والتدقيق للسياســات؟ ولماذا يُعد هذا النشــاط مهماً قبل تطبيق السياسات؟

١٥. ما عملية مراجعة السياسات؟ ومتى تتم عادة؟ وما فائدتها؟

١٦. مــا الامتثال؟ ولماذا هــو ضروري؟ وما هي بعض القوانين التي يجب على منظمتك الامتثال لها؟ (وللإجابة عن هذا الســؤال، اعتبر المنظمة التعليمية التي تدرس فيها هي منظمتك في حال لم تكن موظفاً حالياً).

١٧. ما الفرق بين الامتثال والأمن؟

١٨. مــا الآثار المترتبة على الامتثال لقانون (HIPAA) وذلك فيما يتعلق بأخصائيي أمن المعلومات؟

١٩. مــا الآثار المترتبة عــلى الامتثال لقانون (GLB) وذلك فيــما يتعلق بأخصائيي أمن المعلومات؟

٢٠. مــا الآثار المترتبة على الامتثال لقانون (FERBA) وذلك فيما يتعلق بأخصائيي أمن المعلومات؟

٢١. مــا الآثار المترتبــة على الامتثال لقانــون (SOX) وذلك فيما يتعلق بــالإدارة العليا للمنظمات؟

٢٢. مــا الآثار المترتبة على الامتثال لقانون (HIPAA) وذلك فيما يتعلق بأخصائيي أمن المعلومات؟

٢٣. ما سياسة الاستخدام المقبول؟

٢٤. ما سياسة التشفير؟

٢٥. حدِّد ما إذا كان يجب اعتبار النص في الفقرة التالية على أنه مبدأ توجيهي، أو المرور بالعملية على أنها معيار. علل إجابتك

«جميــع الأنظمة التي تحفظ أرقــام الضمان الاجتماعي يجب تســجيلها في إدارة أمن المعلومات».

أسئلة على نموذج الحالة:

1. ما أحكام القانون الأمريكي رقم «982(B) (2) (a)» ورقم «982(1) (b)»؟
٢. ما الجرائم التي ارتكبها المهاجمون كما وردت في لائحة الاتهام؟
٣. بناءً على هذا الحادث الأمني، ما التوصيات ذات العلاقة بالسياســات والتي تقترحها للشركة لتجنب الأضرار الناتجة عن هجمات مماثلة في المستقبل؟

نشاط التدريب العملي - صياغة سياسة الاستخدام المقبول (AUP):

(من المستحسن تشكيل مجموعة من الطلاب لإكمال هذا النشاط).

قم مع مجموعتك بصياغة سياســة الاستخدام المقبول للحسابات الإلكترونية في جامعة ولاية الشمس المشرقة. وعند تشكيل تلك السياسة، خذ بعين الاعتبار النقاط التالية:

١. ســيتم تطبيق السياسة على جميع الحسابات الإلكترونية التابعة للطلاب والموظفين وأعضاء هيئة التدريس في جامعة ولاية الشمس المشرقة.
٢. يجب أن تتضمن السياســة قائمة بالأنشــطة الممنوعة على الحسابات الإلكترونية في جامعة ولاية الشمس المشرقة.
٣. يجب أن تتضمن السياســة القوانين و/أو التنظيمات التي تؤثر في الاستخدام المقبول لحسابات النظام.
٤. يجب أن تتضمن السياسة عواقب الانتهاك.

وعند الانتهاء مع مجموعتك من صياغة السياسة، احفظها في آلة لينكس الافتراضية كما يــلي: (home/shared/business_finanee/information_technology/website/it//
policy.html) والتي يمكن عرضها على الرابط (http://it.sunshine.edu/policy.html).

قــم بصياغة ملخص للسياســة في ثلاثة إلى أربعة أســطر بحيث يكون مناســباً لتحذير المســتخدمين عند تســجيل الدخول على النظام واحفظ الملخص على الشــكل التالي (etc//
motd). وتأكد من تضمين الرابط الإلكتروني للسياســة حتى يتمكن المســتخدم من قراءة النص الكامل لها.

> إن ملف (/etc/motd) هو ملف «رسالة اليوم» (Message of the Day). وهو ملف نصي يتم طباعته للمستخدمين عند تسجيلهم للدخول، وذلك لنقل الرسائل الهامة مثل المبادئ التوجيهية للاستخدام المقبول.

افتح نافذة طرفية جديدة وقم باستخدام «خادم القشرة الآمنة» (SSH) لعرض «رسالة اليوم»:

```
[root@sunshine ~]# ssh alice@sunshine.edu
```

النتائج المطلوب تسليمها:

١. نسخة من ملف (policy.html).

٢. نسخة من ملف (etc/motd).

تمرين التفكير النقدي - المُبرمج آرون سوارتز (Aaron Swartz):

كان آرون سوارتز (Aaron Swartz) مبرمجاً ماهراً للغاية ويحظى باحترام كبير. وعندما كان عمره ١٤ عاماً، كان واحداً من المؤسســين لخدمة (RSS) المنتشرة، وهي خدمة تسمح للمستخدمين بمتابعة المحتوى من مختلف المواقع الإلكترونية. وكان لدى هذا المبرمج رغبة جامحة بتجاوز حاجز الرســوم المالية من أجل الحصول على المعلومات، وذلك حتى يتمكن

المستخدمون من الوصول إلى المعلومات مجاناً. وللأسف فإن هذه الرغبة الجامحة أدت به إلى تحميل محتويات المكتبة الرقمية (JSTOR) بشكل سري، وذلك باستخدام شبكة معهد ماساتشوستس للتكنولوجيا (MIT). وقام بتحميل ما يقارب من ٤٫٨ مليون مقال على الرغم من المحاولات المتكررة لمنعه.

وأدى هذا الحادث إلى المحاكمة الجنائية بموجب قانون «الاحتيال وإساءة استخدام الحاسب الآلي» (Computer Fraud and Abuse Act)، وبطلب من النيابة العامة ذهب (Aaron) إلى السجن كجزء من اتفاق مع الادعاء العام. وقد عانى (Aaron) لفترة طويلة من الاكتئاب، ولم يكن قادراً على التعامل مع تلك الضغوط، حتى عثر عليه ميتاً في شقته في الثاني عشر من شهر يناير من عام ٢٠١٣. وعُدت حالة الوفاة هذه حالة انتحار.

وقد أدت وفاة هذا المُبرمج إلى ضغوط كبيرة تهدف إلى مراجعة قانون «الاحتيال وإساءة استخدام الحاسب الآلي». وكان المؤيدون لهذا المُبرمج مذعورين لأن عبقرياً كـ (Aaron Swartz) دُفع إلى الموت لمجرد انتهاكه لسياسات الاستخدام المقبول والاتفاقات التعاقدية الأخرى. وقام نائب مدينة (San Jose) ويُدعى (Zoe Lofgren) بتأسيس مشروع قانون أُطلق عليه اسم هذا المُبرمج (Aaron›s law). ويمنع القانون المقترح الملاحقة القضائية بموجب قانون «الاحتيال وإساءة استخدام الحاسب الآلي» عند انتهاك سياسات الاستخدام المقبول أو انتهاك الالتزامات التعاقدية الأخرى في حال كان الانتهاك الأساس الوحيد في تحديد حدوث الوصول غير المصرح.

كما يرى خبراء آخرون أن جريمة هذا المُبرمج لم تكن مجرد انتهاك لسياسات الاستخدام المقبول فحسب، فقد تغلب هذا المُبرمج خلسة على محاولات المكتبة الرقمية (JSTOR) ومعهد ماساتشوستس للتكنولوجيا (MIT) لإيقاف التنزيلات المستمرة، ومن ثم فإنه مذنب بسبب هذا العرض غير الحقيقي.

المراجع:

(هناك العديد من المقالات حول المُبرمج (Aaron Swartz) على شبكة الإنترنت. وفيما يلي المصادر الرئيسية لهذه الحالة)

Schwartz, J. «Internet activist, a creator of RSS, is dead at 26, apparently a suicide,» New York Times, 01/12/2013
Sellars, A. «The impact of 'Aaron's Law on Aaron Swartz's case,» 01/18/2013, http://www.dmlp.org/blog/2013/impact-aarons-law-aaron-swartzs-case (accessed 07/16/2013)
Healey, J. «One bit of Aaron Swartz's legacy: Fixing a bad law?» Los Angeles Times, 01/16/2013
Computer Fraud and Abuse Act, http://www.law.cornell.edu/uscode/text/18/1030 (accessed 07/16/2013)

أسئلة على تمرين التفكير النقدي:

١. هل تعتقد أن موت (Aaron Swartz) كان بسبب تجاوز الادعاء العام؟

٢. على فرض أنك المُدعي العام في هذه القضية، هل ستقوم بشيء مختلف؟ على سبيل المثال، هل ستقوم بفرض عقوبة مخففة نظراً لمساهمات هذا المبرمج في المجال التكنولوجي؟

تصميم حالة:

في أحد الاجتماعات التي ضمت مدققين على مستوى الولاية ومسؤولين من الجامعة، لاحظت أن العديد من العُمداء والمُديرين في جامعة ولاية الشمس المشرقة يستخدمون الأجهزة اللوحية والهواتف الذكية بشكل مكثف. وليس ذلك فحسب فقد لاحظت أيضاً أنهم يستخدمون تطبيقات مثل (Google Drive) و(Dropbox) لنقل المستندات من جهاز إلى آخر بسهولة. وقد نقلت ملاحظاتك إلى عميد كلية إدارة الأعمال الذي يجلس بجانبك في هذا الاجتماع.

اكتب سياسة بشأن حفظ بيانات الجامعة باستخدام التخزين الشخصي المعتمد على الحوسبة السحابية. ويجب أن تحتوي السياسة على لمحة عامة، ونطاق، وتعريفات، وبيان السياسة، وإلزام التنفيذ. وفي الحد الأدنى، خذ بعين الاعتبار النقاط التالية:

- سيتم تطبيق السياسة فقط على كلية إدارة الأعمال.
- هـل الإرشـاد العام أن يقـوم (أو لا يقوم) المسـتخدم بحفظ البيانات باسـتخدام تطبيقات الحوسبة السحابية؟ علل إجابتك.
- هل هناك أي نوع من البيانات يجب ألا يحفظ إطلاقاً في حسابات الحوسبة السحابية الشخصية؟
- هل ستكون إجراءات إلزام التنفيذ لأعضاء هيئة التدريس مختلفة عن إجراءات إلزام التنفيذ للطلاب؟

وبالإضافة إلى السياسة، لخص شروط الخدمة (Terms of Service) لاثنتين من خدمات التخزين السـحابية الشـخصية، مع الإشـارة إلى المشـكلات المحتملة التي قد تجلبها هذه الشروط للجامعة وللمستخدم، متضمناً ذلك المسؤولية المحدودة، وقيود الجاهزية، وغيرها.



الفصل الرابع عشر

تحليل مخاطر تقنية المعلومات وإدارة المخاطر

نظرة عامة:

يدمج هذا الفصل معظم المفاهيم التي ناقشـناها في الفصول السـابقة في إطار شـامل للتعامل مع أمن المعلومات. ففي الفصول السابقة اتبعنا منهجاً تفصيلياً لمناقشة المفاهيم الفرديـة لأمـن المعلومات. لكن في هذا الفصل سـنتبع منهجاً شـمولياً آخذين في الاعتبار تخوفات المجتمع والإدارة العليا وعلاقتها بأمن المعلومات؛ لأن هذه الفئات من المستفيدين تكون أقل اهتمامـاً بالتكنولوجيا وأكثر اهتماماً بتقليل الآثـار الاقتصادية لأمن المعلومات. وتنظـم «إدارة مخاطر تقنية المعلومات» جميع المسـائل المرتبطة بأمن المعلومات، وذلك باستخدام مدخلات من خبراء التقنية وكذلك من خبراء الإدارة.

وتحظى القضايـا الهامة لـلإدارة العليا عادة بالكثير مـن الاهتمام من جهات عديدة. وقـد أدى اهتمام الإدارة العليا بـإدارة المخاطر إلى ظهور العديد مـن نماذج إدارة مخاطر تقنية المعلومات[1]. وسـنقوم في هذا الفصل بجولة سريعة على هذه النماذج، ثم سـنقوم باسـتخلاص الأفـكار من هذه النماذج لإنشـاء نموذج لإدارة المخاطر ينسـجم مع النماذج المعيارية التي اسـتخدمناها للمفاهيم التي ناقشـناها في الفصول السابقة. وفي نهاية هذا الفصل يجب أن تعرف:

- أهمية إدارة المخاطر للإدارة العليا.
- نماذج إدارة مخاطر تقنية المعلومات.
- تحليل المخاطر - التحديد والتقييم.
- إدارة المخاطر - التقليل من المخاطر والاعداد والاستجابة لها.

---

(١) وعلى الرغم من ذلك، فقط (٥٪) إلى (٢٥٪) من شركات فورتشن ٥٠٠ (Fortune ٥٠٠) مستعدة للتعامل مع الأزمات. وهذه الشركات المستعدة للأزمات عادة ما تواجه أزمات أقل بنسبة (٣٣٪)، وتعيش فترة أطول بنسبة (٢٥٪)، ولديها ضعف العائد على الأصول وسمعتها أفضل من الشركات غير المستعدة للأزمات والتي تتفاعل مع الأزمات فقط عند حدوثها. Mitroff, I. I. and M. C. Alpaslan (2003). «Preparing for evil.» Harvard Business Review) (.115-2003(April): 109

مقدمة:

الخطــر هو مقياس كمــي للأضرار المحتملــة الناتجة عن تهديد محــدد. وفي الفصول السابقة قمنا بإعداد القاعدة المعرفية اللازمة لتحليل وإدارة المخاطر. وفي الفصل السادس ناقشنا موضوع التهديدات بالتفصيل. ويمكننا البناء على تلك الأفكار في هذا الفصل لمناقشة قضية تهم الإدارة العليا - وهي إدارة المخاطر.

ولأن إدارة المخاطــر موجهــة من قبل مخــاوف الإدارة العليا، ســنناقش في هذا الجزء التمهيدي موضوع إدارة المخاطر ضمن الســياق العام لإدارة المنظمة. بعد ذلك ســنناقش نماذج إدارة المخاطر المعيارية الموضوعة من قبل المعهد الوطني للتقنية والمعايير (National Institute of Standards and Technology)، والمعــروف اختصــاراً (NIST)، لتوجيــه أنشطة إدارة مخاطر تقنية المعلومات.

إدارة المخاطر بوصفها عنصراً من عناصر الإدارة التنظيمية:

يتم تقييم أداء المنظمة باستخدام مقاييس الربحية. فالمنظمات الأكثر ربحية تكون أكبر قيمــة من تلك المنظمات الأقل ربحية(٢). وبناءً على ذلك فإن التركيز الرئيسي للمديرين هو تعظيم أرباح منظماتهم. ويمكن أن نكتب هذا الاهتمام الإداري على النحو التالي:

موضوع قرار المدير = تعظيم (الربح) = تعظيم (الإيرادات - التكاليف)

ويمكــن للمديرين إنجاز هذا الهدف عن طريق اســتخدام مزيج مــن زيادة الإيرادات (عادة عن طريق رفع الأســعار أو بيع المزيد من الوحدات) أو عن طريق خفض التكاليف. والكثير من أدبيات الإدارة ومعظم المناهج الدراسية لدرجة ماجستير إدارة الأعمال (MBA) مخصصة لتوجيه المديرين لتحقيق هذه الأهداف. ولكن عند التشــغيل اليومي للمنظمات يواجه المديرون أشياء غير عادية تحدث في كل وقت، ويؤثر كثير منها تأثيراً كبيراً في معادلة تعظيم الربح للمنظمة. على ســبيل المثال، لقد رأينا ســابقاً كيف أن الظروف كلفت شركة (TJ Maxx) ١١٨ مليون دولار للتعامل مع تداعيات حادث البطاقات الائتمانية. ويجب أن تُدار هذه الحوادث بشــكل جيد لأنها تؤثر في ربحية المنظمة. وعلى مستوى عالٍ جداً فإن

(٢) لا تهدف جميع المنظمات للربحية. المنظمات غير الربحية مثل الجامعات تمثل قطاعاً كبيراً في الاقتصاد، حيث تمثل أكثر من ١٠٪ من جميع الوظائف في الولايات المتحدة الأمريكية (http://www.urban.org/nonprofits/index.cfm). وفي حين أن هذه المنظمات تقيس مخرجاتها باستخدام معايير مثل عدد الطلبة الخريجين وعدد براءات الاختراع التي تم الحصول عليها، فإن هذه المنظمات تهتم أيضاً بالاستخدام الأمثل لمواردها، ويهتم مديرو هذه المنظمات بنفس اهتمامات المخاطر التي يهتم بها المديرون في المنظمات الربحية.

إدارة التأثـيرات المالية للأحداث غير العادية تُسـمى بإدارة المخاطر. ولتمثيل هذه النقطة يمكننا تعديل موضوع قرار المدير على النحو التالي:

تعظيم (الإيرادات - التكاليف - Δ) وهذا الرمز Δ يعني (دلتا) ويشير إلى تأثير الأحداث غير العادية في المنظمة[٣].

وبشكل عام هناك طريقتان لإدارة المخاطر: (١) جعل المخاطر قابلة للتنبؤ، (٢) التقليل من المخاطر والإعداد لها.

والطـرق العامة لجعـل المخاطر قابلة للتنبـؤ هي التأمين والتحـوط. وهذه من أهم أنشطة القطاع المالي في الاقتصاد. على سبيل المثال، شراء تأمينٍ لحماية مركز البيانات الخاص بك من الفيضانات يجعل من الأثر المالي لحدَث الفيضان قابلاً للتنبؤ والذي يساوي القسط السـنوي المدفوع لشراء التأمين. وعلى الرغم مـن أن الفكرة تبدو غير عادية، إلا أنه يجب أن نؤكـد اعتبار هذا العنـصر عنصراً هاماً في إدارة مخاطر تقنية المعلومات. ونحن (مؤلفو هذا الكتاب) لسـنا خبراء في تصميم وتسـعير الأدوات المالية، لـذا فإننا نترك تفاصيل هذه الطريقـة للخبراء في مجال التمويل. لكن نرغـب في التأكيد على أن الإدارة العليا يجب أن تفهـم هـذه الطريقة جيداً وتأخذها دائماً على محمل الجـد. لذا لا ينبغي أن تندهش إذا سمعت مصطلح «تأمين» في سياق إدارة مخاطر تقنية المعلومات.

وهذا يتركنا مع الطريقة الثانية وهي التقليل من المخاطر والإعداد لها، وهو ما سنناقشه في بقية هذا الفصل.

> تصنيـف آخر مثير للاهتمام هو تصنيف الهجوم والدفاع. فجميع الفرق الرياضية لديها مزيج بين الهجوم والدفاع. وفي نطاق عملنا، تستثمر المنظمات في تقنية المعلومات لتكون وسيلة هجومية فـي المعادلة الربحية لمهاجمـة التكاليف والتعقيد أو للمحاربة للحصول على العملاء في العديد من الأسواق. أما أمن المعلومات فهو الذراع الدفاعي في المعادلة حيث يركز أمن المعلومات على ضمان عدم ضياع الميزة التنافسية الحالية بسبب تطبيقات تقنية المعلومات غير الملائمة [٤]، [٥].

---

(٣) Δ يعني دلتا وهو مصطلح من مصطلحات الصناعة يشير إلى الانحراف عن السلوك العادي.

(٤) أحد طلابنا لخص لنا هذه الفكرة بتذكيرنا بالاقتباس التالي «الهجوم يبيع التذاكر، والدفاع يفوز بالبطولات».

(٥) وموضوع آخر ذو صلة هو ضمان الإدارة الجيدة للمخاطر الجديدة التي تنشأ في المنظمة بسبب استثمارات تقنية المعلومات. على سبيل المثال، بعض الخسائر المالية المثيرة للانتباه حدثت بسبب التداول المالي السريع الذي تم تفعيله بواسطة أنظمة تقنية المعلومات. وهذه النقطة أيضاً لن نناقشها في هذا الفصل. لكن بالإمكان الاطلاع على مناقشة جيدة في المرجع التالي (Westerman, G. and Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage (Hardcover). Boston, MA, Harvard Business School Press)

وبعــد الاطــلاع على هذه الخلفيــة، بإمكاننا الآن مناقشــة نمــاذج إدارة مخاطر تقنية المعلومات والتي تم تطويرها بواسطة المعهد الوطني للتقنية والمعايير (NIST).

الإبلاغ القانوني لعوامل المخاطر بواسطة الإدارة العليا

ومثال على أهمية إدارة المخاطر للمسؤولين التنفيذيين، هناك قانون يلزم الشركات المتداولة علناً بإبلاغ المساهمين عن عوامل المخاطر التي تواجه الشركة.

البند (IA) عوامل المخاطر[٦].

تحت عنوان «عوامل المخاطر»، وحيثما كان مناســباً، تُوضَح عوامل المخاطرة المبينة في بند (503-c) مــن اللائحة رقــم (S-K 229.503-c) من هذا الفصل والتي تنطبق على المســجل. تقديــم أي مناقشــة لعوامل المخاطر بلغة إنجليزية ســهلة وفقاً للمــادة (421-d) من قانون الأوراق المالية لعام ١٩٣٣ رقم (230.421-d) من هذا الفصل. وشــركات الإبلاغ الصغرى ليس مطلوباً منها تقديم المعلومات التي يتطلبها هذا البند.

مــن قانون رقم (229.503-c)[٧]، عوامــل المخاطر للأوراق المالية الصادرة حديثاً تشــمل من بين الأمور العديدة، ما يلي: (١) عدم وجود تاريخ التشــغيل، (٢) عدم وجود عمليات مُربحة فــي الفترات الزمنية الأخيرة، (٣) الموقف المالي، (٤) الأعمال التجارية المقترحة، أو (٥) عدم وجود ســوق للأوراق المالية المشــتركة أو الأوراق المالية القابلة للتحويل لممارسات الأوراق المالية المشتركة.

مثال: (AAPL 10-K) (٣١، أكتوبر، ٢٠١٢)[٨]:

في التقرير الشامل للأداء (K-١٠) لشركة أبل والمُقدم في تاريخ (٢٠١٢/١٠/٣١)، من بين عوامل المخاطر الأخرى، ذكرت شركة أبل العاملين التاليين والمرتبطين مباشرة بتقنية المعلومات:

قد تتأثر أعمال الشركة وسمعتها بسبب فشل نظام تقنية المعلومات أو تعطل الشبكة.

قــد تكون الشــركة مُعرضة لاختراقات في نظم تقنية المعلومــات التابعة لها، وهو ما قد يضر بشركاء العمل وعلاقات العملاء أو التأثير سلباً في الوصول للخدمات الإلكترونية ومتجر الشراء على الإنترنت، كما يمكن أن تتعرض الشركة لعواقب قانونية وتشغيلية ومالية وخيمة، ويمكن أن تتعرض أيضاً لعواقب تضر بسمعة الشركة.

---

(6) http://www.sec.gov/about/forms/form10-k.pdf

(7) http://www.law.cornell.edu/cfr/text/17/229.503

(8) http://investor.apple.com/

نماذج إدارة المخاطر:

النمــوذج هو هيكل لدعم شيء آخر. وفي أدبيات الإدارة تُســتخدم النماذج عند وجود عدد كبير من الأفكار التي تحتاج إلى تنظيم بطريقة يســهل فهمها وحفظها من قبل الكثير من الأشــخاص. مثــلاً، أطر الإدارة تدعم المنظمة وذلك فيما يتعلــق بالمفاهيم ذات الصلة لتحقيق الأهداف المرجوة.

وهنــاك الكثير من النماذج المشــهورة لإدارة المخاطر متضمناً ذلك نموذج (OCTAVE) التابع لمعهد هندسة البرمجيات (SEI)، ونموذج (ISO 27002) التابع لمنظمة المعايير الدولية، والمبادئ التوجيهية في إدارة مخاطر المعلومات والتابعة للمعهد الوطني للتكنولوجيا والمعايير (NIST 800- 39). وبالإضافــة إلى ذلك فإن الشركات الرائدة مثل شركة مايكروســوفت[٩] وشركة جوجــل[١٠] قامتا بإصدار توصياتها الخاصــة لإدارة مخاطر أمن المعلومات. وجميع هذه المبادئ التوجيهية تقدم أفكاراً متشابهة، كما تمثل تلك المبادئ نتائج للجهود الجماعية لأفضــل العقــول في هذه الصناعة، وذلــك لإدارة مخاطر تقنية المعلومــات. وأي من هذه المبادئ التوجيهية يُعد أساساً ممتازاً لوضع خطة إدارة المخاطر في المنظمة.

مــن المستحســن اعتماد واحد من نمــاذج إدارة المخاطر الموحدة وذلــك لوضع خطة إدارة المخاطر مع إجراء التعديلات الخاصة بسياق المنظمة. وعموماً فإن وضع خطة لإدارة المخاطر من الصفر يُعد فكرة ســيئة، لأنه من المحتمل جداً نســيان العديد مــن الموضوعات المهمة، والتي ستكتشــفها بتكلفة كبيــرة على المنظمة، وذلك حينما يكشــف أحــد التهديدات ذلك الإهمــال في نموذج إدارة المخاطر. وقد يكون من الحكمــة أن نتذكر قول بنيامين فرانكلين (Benjamin Franklin) في هذا الشأن «الخبرة مدرسة ثمينة، إلا أن الحمقى ليس لهم طريقة أخرى للتعلم».

ونفضــل في هذا الكتاب أن نســتعرض أفكارنا بطريقة متناســقة عبر الفصول لأن هذه الطريقة تســهل الفهم والتذكر. وقد وجدنــا أن المبادئ التوجيهية التابعة للمعهد الوطني للتكنولوجيا والمعايير (NIST 800- 39) هي الأنســب لهــذا الغرض لأنها متوافقة جداً مع

(9) http://technet.microsoft.com/en-us/library/cc163143.aspx

(10) https://cloud.google.com/files/Google-CommonSecurity-WhitePaper-v1.4.pdf

الطريقة التي عرضنا بها المعلومات في الفصول الســابقة. وبناءً على ذلك ســنركز على هذه المبــادئ التوجيهية فيما تبقى من هــذا الفصل. كما قمنا بدمج العديــد من الأفكار التي ناقشــناها في الفصول الســابقة (مثل نموذج المخاطر ودورة حياة الكوارث) في نموذج إدارة المخاطر التابع للمعهد الوطني للتكنولوجيا والمعايير. وللتأكد من اكتمال الفكرة، ســنعرض لمحة سريعة عن بقية النماذج الشائعة في نهاية هذا الفصل.

نموذج إدارة المخاطر التابع للمعهد الوطني للتقنية والمعايير (NIST 800-39):

أصــدر المعهد الوطني للتقنية والمعايــير توصياته الخاصة بإدارة مخاطر أمن المعلومات في إصــدار خاص رقم (٨٠٠-٣٩)[١١]. ويرجع تاريخ الإصدار الحالي إلى شــهر مارس من عام ٢٠١١. وهذه المبادئ التوجيهية تم تطويرها من خلال مدخلات من المجتمع الاســتخباراتي والدفاعي والمدني، وذلك لتقديم نموذج أمن المعلومات للحكومة الفيدرالية. وهذه المبادئ التوجيهية (وكذلك النقاش في هذا الفصل) عامة جداً ولا تهتم بالموضوعات المحددة التابعة لبيئــات أمنية عالية مثل القواعد العســكرية أو القوانين الخاصة مثــل قانون (HIPAA). وهذه البيئات تستخدم إجراءات أكثر صرامة من تلك المقترحة في (NIST 800 -39). لكن نمــوذج (NIST 800- 39) مفيد جداً لغالبية المنظــمات التجارية والمنظمات غير الربحية، ومــن ثم فإن هذا النموذج مناســب لأغراض هذا الكتــاب. وإذا كنت تعمل في بيئة أمنية عالية مثل قاعدة عســكرية أو بنك، فإن المنظمة ستُقدم لك مبادئ توجيهية إضافية لإدارة المخاطر الخاصة بتلك البيئة.

ويمكن تعريف مخاطر تقنية المعلومات بأنها المخاطر المرتبطة باستخدام نظم المعلومات في المنظمة. وهذا واحد من العديد من المخاطر التي تواجه المنظمة. ويؤكد المعهد الوطني للتقنيــة والمعايير (NIST) على أن إدارة المخاطر ليســت علــماً دقيقاً، بل هي أفضل حكم جماعي من الأشــخاص في الرُتب والوظائف حول التدابير المناسبة لحماية المنظمة. ويوصي نمــوذج (NIST 800- 39) بأن تشــارك الإدارة العليا في إدارة مخاطر تقنية المعلومات، وأن يتم دمج مخاطر إدارة مخاطر تقنية المعلومات في تصميم عمليات المنظمة[١٢].

---

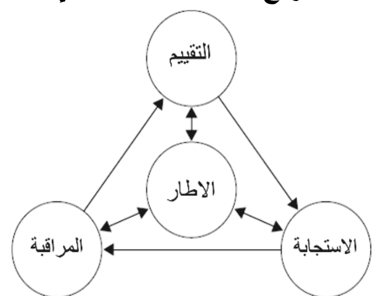
(11) http://csrc.nist.gov/publications/nistpubs/800-39/SP800-39-final.pdf (accessed 12/20/2012)

(12) رابط عن مخاطر تقنية المعلومات وهو مفيد جداً لمسؤولي المدارس (.http://dangerouslyirrelevant Appeared in Bruce .(2013/22/26-internet-safety-talking-points.html (accessed 07/08/org/2012 (2012/15/Schneier's blog, 9

عناصر إدارة مخاطر تقنية المعلومات:

يحــدد نموذج (NIST 800-39) أربعة عناصر لإدارة مخاطــر تقنية المعلومات - (١) إطــار المخاطر، (٢) تقييم المخاطر، (٣) الاســتجابة للمخاطر بعــد تقييمها، (٤) المراقبة المستمرة للمخاطر اعتماداً على الخبرات المكتسبة من أنشطة الاستجابة للمخاطر. وهذه العناصر مرتبة كما هو في الشكل (١٤-١).

الشكل (١٤-١): نموذج (NIST 800 -39) لإدارة المخاطر



إطار المخاطر يحدد الســياق لإدارة المخاطر من خلال وصف البيئة التي يتم فيها اتخاذ القــرارات على أســاس المخاطر. وهذا يوضــح لجميع الأعضاء في المنظمــة معايير المخاطر المختلفة والمســتخدمة في المنظمة. وتشــمل هــذه المعايير ما يــلي: (١) افتراضات حول المخاطر التي تُعد مهمة، (٢) الاســتجابة التي تُعد عملية، (٣) مستويات المخاطر التي تُعد مقبولــة، (٤) الأولويــات والمفاضلة عند الاســتجابة للمخاطر. وإطــار المخاطر يُحدد أيضاً المخاطر التي يتم إدارتها من قبل القادة/ المديرين التنفيذيين.

> وفي مثال تقليدي لإطار المخاطر الذي تم تســليط الضوء عليه خلال المناقشات الرئاسية عام ٢٠١٢ هــو وجود إشــارة واحدة فقط للإرهــاب في خطاب رئيس الولايات المتحدة للشــعب الأمريكي عام ٢٠٠١. وفي العام التالي، أي بعد هجمات ١١/٩، كان هناك ٣٦ إشــارة للإرهاب في خطاب رئيس الولايات المتحدة للشعب الأمريكي عام ٢٠٠٢.
>
> ألا يعــد ذلك تغيــراً واضحاً في إطار المخاطر للجناح التنفيذي فــي حكومة الولايات المتحدة الأمريكية خلال عام واحد فقط؟

وفي سياق إطار المخاطر، تعمل عناصر تقييم المخاطر على تحديد جميع المخاطر التي تواجه المنظمة وتجميعها. وكما تذكر فقد عرفنا المخاطر بأنها مقياس كمي للضرر المحتمل من التهديد. ويقوم تقييم المخاطر بتطوير تلك التقديرات الكمية من خلال التعرف على التهديدات والثغرات والضرر على المنظمة في حال استغلت التهديدات تلك الثغرات. وسنناقش تقييم المخاطر بمزيد من التفصيل في الجزء التالي.

أما الاستجابة للمخاطر فتتناول كيفية استجابة المنظمات للمخاطر بمجرد تحديدها بواسطة تقييم المخاطر. وتساعد الاستجابة للمخاطر في تطوير استجابة متسقة على مستوى المنظمة والتي بدورها تكون متسقة مع إطار المخاطر. وباتباع إجراءات العمل الموحدة، تتكون الاستجابة للمخاطر مما يلي: (١) وضع مسارات بديلة للعمل من أجل الاستجابة للمخاطر، (٢) تقييم تلك المسارات البديلة، (٣) اختيار مسار العمل المناسب، (٤) تنفيذ الاستجابة للمخاطر اعتماداً على مسار العمل الذي تم اختياره.

ويعمل عنصر مراقبة المخاطر على تقييم فاعلية خطة إدارة المخاطر للمنظمة مع مرور الوقت. وتشمل مراقبة المخاطر على ما يلي: (١) التحقق من تنفيذ تدابير الاستجابة للمخاطر المخطط لها، (٢) التحقق من أن الاستجابة المخطط لها تلبي المتطلبات المستمدة من رسالة المنظمة ووظائف العمل واللوائح والمعايير، (٣) تحديد فاعلية تدابير الاستجابة للمخاطر، (٤) تحديد التغييرات المطلوبة في خطة إدارة المخاطر نتيجة للتغييرات في التكنولوجيا وبيئة العمل.

والأسهم في الشكل (١٤-١) توضح عمليات إدارة المخاطر وتدفق المعلومات والتواصل بين عناصر إدارة المخاطر. والأنشطة الموضحة في الدوائر الخارجية يتم تنفيذها بالتتابع، وذلك بالانتقال من تقييم المخاطر إلى الاستجابة للمخاطر إلى مراقبة المخاطر. أما إطار المخاطر فيعمل على تغذية جميع الأنشطة المتتابعة خطوة بخطوة. على سبيل المثال، التهديدات المُحددة من إطار المخاطر تكون بمثابة مدخلات لنشاط تقييم المخاطر. وبالمثل فإن مخرجات عنصر تقييم المخاطر تكون بمثابة مدخلات لعنصر الاستجابة للمخاطر[١٣].

(١٣) تحتوي وثيقة نموذج (NIST 800-39) على أسهم ثنائية الاتجاه في كل مكان في الشكل. لكننا استخدمنا أسهماً موجهة لربط الدوائر الخارجية. ونعتقد أن ذلك يوضح بشكل أفضل طبيعة الأنشطة المتتابعة وتدفق المعلومات من تقييم المخاطر إلى الاستجابة إلى المراقبة.

تقييم المخاطر:

وبمجرد أن يتم وضع إطار المخاطر، يمكننا أن نُصمم نموذجاً لتقييم المخاطر اعتماداً على نموذج التهديد الذي صُمم سابقاً.

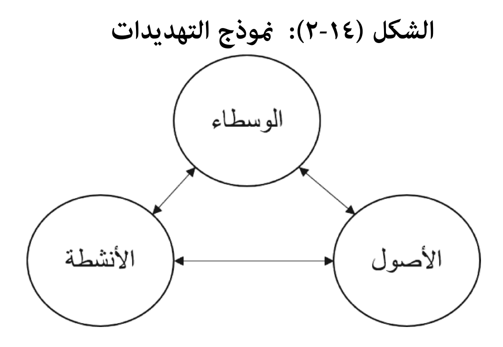
إزالة الغموض عن تقييم المخاطر وتحليل المخاطر

يحتوي عنصر تقييم المخاطر في نموذج (NIST 800-39) على نشاطين وهما: تحديد المخاطر وقياس هذه المخاطر. وما يُطلق عليه «تقييم المخاطر» في هذا النموذج يُطلق عليه أيضاً «تحليل المخاطر»، حيث تشير عبارة «تقييم المخاطر» إلى الجانب الكمي من عنصر تقييم المخاطر في نموذج (NIST 800-39). ويساعد السياق في إزالة الغموض عن معنى عبارة «تقييم المخاطر».

نموذج تقييم المخاطر:

يوضح الشكل (١٤-٢) نموذج التهديد الذي ناقشناه سابقاً. والتهديدات تشمل الوسطاء المُحفزين الذين يهاجمون الأصول. ولا نقوم عادة بإجراء تحليل رسمي للنتائج المحتملة للتهديد أثناء إجراء تحليل التهديدات، فاهتمامنا خلال التحليل يقتصر على تحديد المشكلات المحتملة.

الشكل (١٤-٢): نموذج التهديدات



على سبيل المثال، أحد التهديدات المُحددة هو قرصان حاسب عن بعد (وسيط) يحاول اختراق قاعدة بيانات المستخدم الخاصة ببيانات الاعتماد (أصل) بواسطة سرقة بيانات

الاعتماد تلك (نشاط). وخلال تحليل التهديد، لا ننظر إلى الأثر المحتمل لمثل هذا التهديد. وعلى وجه التحديد، نحن لا نقلق بشأن ما قد يفعله قرصان الحاسب بمثل تلك المعلومات.

ويمكــن أن يُنظــر إلى تقييم المخاطر بأنه إضافة تحليل النتائــج إلى التهديدات التي تم تحديدهــا. وتعريفنا للمخاطر بأنها مقيــاس كمي للضرر المحتمل الناتج عن تهديد محدد يُمكن أن يكتب على النحو التالي:

المخاطر = الضرر الناتج عن تهديد محدد أو

المخاطــر = الضرر (التهديد)، بمعنــى أن المخاطر هي الضرر كمخرجات لدالة مدخلاتها التهديد

ولأن التهديد بذاته يتكون من وســيط ونشاط وأصل، يمكننا كتابة معادلة المخاطر على النحو التالي:

المخاطر = الضرر (الوسيط، النشاط، الأصل)

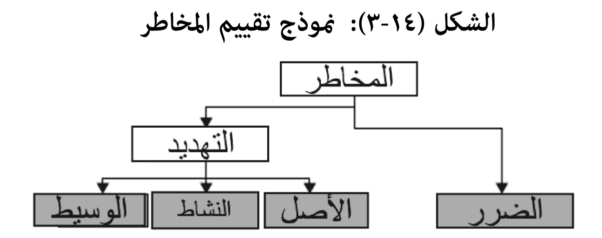
وهذا موضح في الشكل (١٤-٣). ويمكننا استخدام هذا الشكل لتحديد المخاطر وكتابتها على شــكل عبارات تحتــوي على جميع المعلومــات اللازمة لنقل المعلومــات عن المخاطر للأطراف المعنية. ورجوعاً لمثال تهديد قرصان الحاسب الذي سرق بيانات اعتماد المستخدم، نستطيع كتابة المخاطر المرتبطة بهذا المثال على النحو التالي:

خطر ١: قرصان حاســب عن بعد (وســيط) قد يسرق (نشــاط) بيانات اعتماد (أصل) ويستخدم تلك البيانات للوصول إلى المواقع الإلكترونية للبنوك (نشاط). وهذا قد يؤدي إلى دعوى قضائية والتي تستنزف الأموال وكذلك وقت الإدارة (ضرر).

خطر ٢: قرصان حاســب عن بعد (وســيط) قد يسرق (نشــاط) بيانات اعتماد (أصل) ويستخدم تلك البيانات للوصول إلى المواقع الإلكترونية للبنوك (نشاط). وهذا قد يؤدي إلى السمعة السيئة والتي قد تضر أعمالنا على المدى القصير (ضرر).

وبعبارة أخرى فإن التهديد نفســه قد يرتبط بمخاطر متعددة إذا كان التهديد يمكن أن يسبب أشكالاً متعددة من الضرر.

الشكل (١٤-٣): نموذج تقييم المخاطر



ويوضح نموذج تقييم المخاطر في الشكل (١٤-٣) أن مجموعة صغيرة من الأصول والوسطاء قد تؤدي إلى عدد كبير من التهديدات والمخاطر. على سبيل المثال، إن مزيجاً بين اثنين من الوسطاء (مهاجم عن بعد وموظف ساخط) واثنين من الأصول (أصول معلوماتية وأصول الأجهزة) قد تؤدي إلى أربعة تهديدات محتملة. وإذا أضفنا اثنين من الأضرار إلى هذا المزيج (الخسارة المالية، وفقدان المعلومات) يصبح لدينا ثمانية مخاطر محتملة للنظر فيها. وفي العالم الحقيقي فإن أصغر الأعمال تتعامل مع عشرات من الأصول والوسطاء (والتي يمكن أن تكون مدفوعة بدوافع متعددة) والأضرار التي قد تؤدي إلى عشرات الآلاف من المخاطر المحتملة (هذا إذا ضربنا أعداد الوسطاء والأصول والأنشطة والأضرار في بعضها فقط). لكن معظم المنظمات يمكنها التعامل في أي وقت من الأوقات مع ٥ إلى ١٠ مخاطر فقط. وهذا هو سبب أهمية إطار المخاطر - لاستبعاد المخاطر غير المحتملة.

وبمجرد تحديد المخاطر يمكن وضع التدابير الكمية للمخاطر عن طريق تقدير احتمال الأضرار المتوقعة عند حدوث المخاطر. ويمكننا بعد ذلك حساب المخاطر كحاصل ضرب احتمالية الضرر في مقدار الضرر. واستكمالاً لمثال قراصنة الحاسب السابق، لنفرض أن تقدير احتمالية الهجوم في السنة القادمة يساوي (١٪). وللخطر ٢ أعلاه، نقدر الأضرار النقدية من خسارة المبيعات بـ ١٠ آلاف دولار في الأرباح. ويمكننا قياس الخطر في هذه الحالة على النحو التالي:

الخطر = احتمالية الضرر x مقدار الضرر = ٠,٠١ x ١٠,٠٠٠ = ١٠٠ دولار

ومن خلال تطوير تقديرات مماثلة لجميع المخاطر التي تم تحديدها يمكننا ترتيب أولويات المخاطر ضمن إطار المخاطر.

نماذج إدارة المخاطر الأخرى:

يعــد نموذج (NIST 800 - 39) نموذجاً عاماً جداً لإدارة مخاطر تقنية المعلومات. ومن بــين نماذج إدارة مخاطر أمن المعلومات الأكثر انتشــاراً نمــوذج (OCTAVE) التابع لمعهد هندســة البرمجيات (SEI)، ونموذج (ISO 27002) التابع لمنظمة المعايير الدولية. وهناك العديد من الشركات الاستشــارية التي تســاعد المنظمات على تنفيذ توصيات هذه المعايير. ولاستكمال هذه الفكرة نعرض في هذا القسم لمحة موجزة عن اثنين من هذه المعايير.

سلسلة (ISO 27000):

قامــت منظمــة المعايــير الدوليــة (International Standards Organization)، أو اختصاراً (ISO)، بتخصيص سلسلة المعايير (ISO 27000) (أي المعايير التي تبدأ بالرقم ٢٧) لشــؤون أمن المعلومات. واعتباراً من شهر ديسمبر من عام ٢٠١٢، تضمنت هذه السلسلة ســتة معايير تبدأ من معيار (ISO 27001) وتنتهــي بمعيار (ISO 27006). وهذه المعايير تغطي الموضوعات التالية:

(ISO 27001): المعيــار الذي يحدد متطلبات نظــام إدارة أمن المعلومات والمعروف اختصاراً (ISMS).

(ISO 27002): المعيــار الــذي يحــدد مجموعة الضوابط المطلوبــة لتلبية المتطلبات المحددة في معيار (ISO 27001).

(ISO 27003): معيار يقدم توجيهات لتنفيذ نظام إدارة أمن المعلومات (ISMS).

(ISO 27004): معيار يقدم القياس والمؤشرات لنظام إدارة أمن المعلومات (ISMS).

(ISO 27005): معيار لإدارة مخاطر أمن المعلومات.

(ISO 27006): المعيــار الــذي يقدم مبــادئ توجيهية لاعتماد المنظــمات التي تقدم شهادة نظام إدارة أمن المعلومات.

وينــص معيــار (ISO 27001) على تبنــي نهج العمليات لتنفيــذ أمن المعلومات. وجميــع العمليــات تتبع نموذج ديمنــج (Deming's model): خطــط، نفذ، افحص، اســتجب (Plan-Do-Check-Act). خــلال مرحلــة التخطيــط تقوم المنظمــة بصياغة السياســات والإجراءات لإدارة مخاطر المعلومات. ويتم تشــغيل هذه الإجراءات في مرحلة التنفيذ. أما في مرحلة الفحص، فيتم قياس أداء العملية ومقارنتها بما يقابلها من المواصفات المخطط لها، ومن ثم عرضها على الإدارة للمراجعة. وفي مرحلة الاســتجابة، تُستخدم نتائج المراجعة لتحسين السياسات والإجراءات في مرحلة التخطيط من الدورة التالية.

وقد تكون لاحظت أوجه الشــبه بين معيــار (NIST 800- 39) ومعيار (ISO 27001) حيث تتفق مرحلة التقييم في معيار (NIST) مع مرحلة التخطيط في معيار (ISO)، وتتفق مرحلة الاســتجابة في المعيار الأول مع مرحلة التنفيــذ في المعيار الثاني، وكذلك تتفق مرحلة المراقبة من معيار (NIST) مع مرحلتي الفحص والاستجابة من معيار (ISO).

أما معيار (ISO 27002) فيوثق مجموعة من التقنيات الأمنية والتي تتفق مع الضوابط التي ناقشناها في هذا الكتاب. وهذه الضوابط مقسمة للأقسام التالية: (١) إدارة الأصول، (٢) أمــن المــوارد البشرية، (٣) الأمن المــادي والبيئي، (٤) إدارة العمليــات والتواصل، (٥) التحكــم في الوصول، (٦) حيازة نظم المعلومات وتطويرها وصيانتها، (٧) إدارة حوادث أمن المعلومات، (٨) إدارة استمرارية الأعمال، (٩) الامتثال[١٤].

ويحــدد معيار (ISO 27005) أن عملية إدارة مخاطر أمن المعلومات تتكون من ســبع خطوات متتابعة: (1) إنشــاء السياق، (2) تقييم المخاطر، (3) معالجة المخاطر، (4) قبول المخاطر، (5) تنفيذ خطة علاج المخاطر، (6) مراقبة المخاطر ومراجعتها، (7) تحسين عملية إدارة المخاطــر. وباتبــاع توصيات نمــوذج - خطط، نفذ، افحص، اســتجب في معيار (ISO 27001)، فــإن خطوات معيار (ISO 27005) تتفق مع مراحل نموذج ديمنج الأربع كما هو موضح في الجدول (14-1).

(١٤) ناقشنا باختصار في هذا الكتاب موضوع إدارة استمرارية الأعمال. ويرجع ذلك إلى معظم خريجي الجامعات الجدد يكون لديهم مسؤولية محدودة جداً عن استمرارية الأعمال. ولقد اخترنا أن نحافظ على تركيزنا على موضوعات أمن المعلومات الأكثر ملاءمة لخريجي الجامعات ولفترة ٤-٥ سنوات الأولى بعد التخرج.

وكــما ترى فهناك تداخــل كبير بين توصيات معيار (ISO) ومعيــار (NIST) من حيث صلتها بأمن المعلومات.

الجدول (١٤-١): التوافق بين عناصر عملية إدارة نظام أمن المعلومات لمعيار (ISO 27001) وعناصر عملية إدارة مخاطر أمن المعلومات لمعيار (ISO 27005)

مراحل عملية إدارة نظام أمن المعلومات	مراحل عملية إدارة مخاطر أمن المعلومات
التخطيط	إدارة الأصول
	تقييم المخاطر
	تطوير خطة علاج المخاطر
	قبول المخاطر
التنفيذ	تنفيذ خطة علاج المخاطر
الفحص	المراقبة المستمرة للمخاطر ومراجعتها
الاستجابة	تحسين وتطوير عملية إدارة مخاطر أمن المعلومات

نموذج (OCTAVE):

تســتضيف جامعة كارنيجــي ميلــون (Carnegie Mellon) معهد هندســة البرمجيات (Software Engineering Institute) المشــهور، والمعروف اختصــاراً (SEI). وهذا المعهد الممول اتحادياً أخذ على عاتقه على مر الســنين الإشراف على التنســيق في مختلف الأنشــطة المهمــة لصناعة البرمجيات. ولقد بدأ المعهــد ذلك من خلال وضع المبادئ التوجيهية الموصى بها لتحسين عملية تطوير البرمجيات. وفي السنوات الأخيرة، أخذ المعهد القيادة في مجال أمن المعلومات والحفاظ على المســتودع الرئيــسي لتقارير الأخطاء الصادرة من موردي البرمجيات الرئيســيين. وأحــد مبــادرات هذا المعهــد البارزة هــي منهجيــة (OCTAVE) لإدارة أمن المعلومات. و(OCTAVE) هي اختصار لعبارة (Operationally Critical Threat, Asset, Vulnerability Evaluation) والتــي تعنــي «التقييم العملي والحاســم للثغرات والأصول والتهديدات». وتتفق هذه المنهجية مع مرحلة تقييم المخاطر في نموذج (NIST 800- 39).

ووصــف منهجية (OCTAVE) الوارد أدنــاه اعتمد على اللمحة العامة الموجودة في الموقع الإلكتروني لمعهد هندسة البرمجيات[١٥].

وقد تم تطوير منهجية (OCTAVE) للمنظمات الكبيرة (٣٠٠ موظف أو أكثر). وهذه المنظمات في الغالب تملك بنية تحتية لتقنية المعلومات، كما تملك القدرة على إدارة عمليات أمــن المعلومــات الخاصة بها. وتعتمــد منهجية (OCTAVE) على ثــلاث مراحل لفحص الموضوعــات التقنية والتنظيمية مما يعطي صورة شــاملة عن احتياجــات أمن المعلومات للمنظمة. والمراحل الثلاث هي:

مرحلة ١: تحديد الأصول الحرجة وتحديد التهديدات على تلك الأصول.

مرحلــة ٢: تحديد الثغــرات التنظيمية والتقنية والمعرضة لتلك التهديدات والتي تشــكل خطراً على المنظمة.

مرحلة ٣: وضع إستراتيجية حماية قائمة على الممارسات ووضع خطة لتقليل المخاطر، وذلك لدعم رسالة المنظمة وأولوياتها.

وتتضمن منهجية (OCTAVE) سلســلة من ورش العمل، يتــم تنفيذها إما على أيدي خــبراء من الخارج أو من خــلال فريق تحليل متعدد التخصصات يتضمن ٣ إلى ٥ من أفراد المنظمة. وهذه المنهجية تســتفيد من المعرفة الموجودة في المســتويات المتعددة للمنظمة. وتكون هذه الأنشــطة مدعومة بالممارسات الجيدة والمعروفة، ومدعومة كذلك بالدراسات الميدانية وأوراق العمل التي يمكن أن تُســتخدم لاســتنباط المعلومات خلال جلســات حل المشكلات والنقاشات المركزة.

وكما لاحظــت هناك توافق كبير بين نمــوذج (OCTAVE) ونمــاذج إدارة مخاطر أمن المعلومات الأخرى والتي ناقشناها سابقاً (NIST 800- 39, ISO 27000).

ضوابط تقنية المعلومات العامة للامتثال لقانون (Sarbanes-Oxley):

إلى الآن ناقشــنا في هــذا الفصل نماذج عامة لإدارة مخاطــر أمن المعلومات والتي يمكن اســتخدامها في مجموعة واسعة من الصناعات. وفي حين أن هذه النماذج مفيدة في معظم

(15) http://www.cert.org/octave/octavemethod.html (accessed 12/28/2012)

الحــالات، إلا أن هناك متطلبات قانونية محددة لمنهجيــات إدارة مخاطر تقنية المعلومات تظهر في حالات المخاطر العالية جداً. وأحد تلك الحالات إعداد التقارير المالية في الشركات المطروحة للتداول العام. وهذا السياق أصبح دافعاً كبيراً لتوظيف خريجي أمن المعلومات الجــدد في العقد الأخير من الزمن. كما أن هذا الســياق أدخل مصطلحات في قاموس أمن المعلومات مثل قانون (Sarbanes-Oxley) أو اختصاراً (SOX)، وقســم ٣٠٢، وقسم ٤٠٤، والضوابــط الداخلية، وضوابط تقنية المعلومات العامة. ونظراً لهذه الأهمية ســنُقدم لمحة عامة عن هذا السياق في هذا الجزء.

قانون (Sarbanes-Oxley) لعام ٢٠٠٢:

في الســنوات الأخيرة من القرن العشرين، شــهدت أمريكا أشــهر موجــة لارتفاعات الأســهم في التاريخ المالي، فقد أدت فرص الأعمال على الإنترنت بالمســتثمرين إلى المزايدة على أســعار أي شركة مرتبطة بالإنترنت. وعُرفت هذه الظاهرة بـ «فقاعة الدوت كوم» (dot-com boom). ولذا طور المحللون مقاييس لتبرير تلك الأسعار المرتفعة مثل مقياس (dollars per eyeball). وقــد كان الاســتثمار في بعــض الشركات يُعــد مُكلفاً على الرغم من أن أســعار أسهمها قد بلغت أضعاف دخلها الســنوي. وبلغ تقييم ثمن بعض الشركات خــلال ذلك الوقت مليار دولار دون تحقيق أي أرباح، والكثير من الشركات بلغ تقييم ثمنها أكــبر بمائة مرة مــن أرباحها الســنوية. وفي المراحل الأخيرة من هذا الجنــون، وعندما بدأ الناس يتساءلون عن هذه التقييمات العالية وأصبحت الشركات تحت ضغوط لتبرير أسعار أســهمها، قام بعض المديرين التنفيذيين في بعض الشركات المعروفة بتزوير حســاباتهم إما لإظهار مبيعات لم تحدث في الواقع (شركة MCI- Worldcom) أو لإخفاء التكاليف (شركة Enron). والعديد من هؤلاء المديرين التنفيذيين حقق مصالح شخصية من ذلك التزوير.

وعندمــا جاءت هذه الحــالات إلى المحاكمة، نفى قادة تلك الشركات قيامهم بأي ذنب، واعتمدوا على حجة أنهم وقّعوا البيانات المالية اعتماداً في المقام الأول على موظفي المحاسبة والمراجعــين. وقد ادعى هؤلاء القادة بأن عمليات الشركات معقدة جداً بحيث يســتحيل بالنسبة لهم معرفة جميع جوانب البيانات المالية. ومع ذلك، كان خبراء الإدارة والجمهور، والمشرعــين على قناعة بأن هؤلاء القادة يعرفون بالضبط ما كانوا يفعلون وكانت ادعاءاتهم بالجهل محاولة لمجرد استغلال الثغرات القانونية وتجنب العقوبات.

وهذه المحاكمات سلطت الضوء على نقطتين من التفاصيل الهامة لسوق الأوراق المالية. النقطة الأولى هي أن اسـتثمار تقاعـد معظم الأمريكان كان مرتبطاً ارتباطاً وثيقاً بسـوق الأسـهم لأن معظم صناديق التقاعد لا خيار لها سـوى أن تسـتثمر معظم أصولها في سوق الأسهم في الولايات المتحدة لتحقيق النمو المطلوب ولمساعدة الأشخاص على التقاعد بأمان. فعندما قامت الشركات الكبرى مثل شركة (Enron) وشركة (MCI-Worldcom) بالتلاعب بقوائمهـا المالية، ومن ثـم انهارت في نهاية المطاف، أدى ذلـك إلى ضرر أصول التقاعد لكل عامل أمريكي تقريباً. النقطة الثانية هي أن قادة الشركات كان بإمكانهم القيام بالمزيد من المخالفات في شركاتهم من خلال التوجيهات الشـفهية والضمنية والتي لا تترك أثراً ملموسـاً يمكن استخدامه أثناء المحاكمات.

وتحـت الضغط الكبير لاتخاذ الإجراء المناسـب، أصدر مجلـس النواب الأمريكي قانون سـاربينز أوكسـلي (Sarbanes-Oxley) في عام ٢٠٠٢. وسمُي هذا القانون باسم اثنين من رعاته الأساسـيين وهما: السـيناتور (Paul Sarbanes) والنائب (Michael G. Oxley). ويشـير نمط التصويت على الدعم التشريعي الكبير في الوقت الذي أصدر فيه هذا القانون حيـث حصل هذا القانون على ٤٢٣ صوت من ٤٣٤ من الأصوات الممكنة في البيت الأبيض، كما حصل على ٩٩ صوتاً من ١٠٠ من الأصوات الممكنة في مجلس الشيوخ.

ساربينز أوكسلي - أحكام هامة:

من وجهة نظر قانونية، هناك تأثير واحد رئيسي على القانون. فالقسـم (٣٠٢) والقسم (٩٠٦) وضعا أحكاماً جنائية جديدة تجعل المديرين التنفيذيين والمديرين الماليين في الشركات المطروحة للتداول العام مسـؤولين مسؤولية جنائية عن أي بيانات غير صحيحة في الأوراق الرسـمية. ويصبح بذلك المديرون التنفيذيون والمديرون الماليون مسـؤولين بشكل شخصي عن صحة المعلومات المالية الواردة في الأوراق الرسمية. وقبل صدور قانون ساربينز أوكسلي (Sarbanes-Oxley)، كان يجـب على النيابة العامة أن تقـوم بإثبات وجود النية الخبيثة للبيانات غير الصحيحة حتى يمكن اعتبار ذلك جريمة جنائية. وللاطلاع نرفق أدناه الأحكام ذات الصلة من هذا القانون.

مستند (١٤-١) | مقتطفات من قسم ٣٠٢ من قانون ساربينز أوكسلي

قسم ٣٠٢. مسؤولية الشركات عن التقارير المالية.

(أ) التنظيمات المطلوبة - تتطلب الهيئة من كل شركة تقديم تقارير دورية بموجب مادة (١٣أ) أو (١٥د) من قانون الأوراق المالية لعام ١٩٣٤ رقم (U.S.C. 78m, 78o (d 15) وأن المسؤول التنفيذي الرئيسي أو المسؤولين والمسؤول المالي التنفيذي أو المسؤولين أو الأشخاص الذين يؤدون وظائف مماثلة يتعهدون في كل تقرير سنوي أو ربع سنوي يُقدم في إطار هذا القانون بما يلي:

(١) أن يقوم المسؤول عن التوقيع بمراجعة التقرير.

(٢) اعتماداً على معرفة المسؤول، ألا يتضمن التقرير أي تصريحات غير صحيحة لواقعة مادية أو تجاهل لواقعة مادية تكون ضرورية لإصدار التصريحات، في ضوء الظروف التي قُدمت فيها تلك التصريحات، وألا تكون تلك التصريحات مضللة.

(٣) اعتماداً على معرفة المسؤول، أن تكون التصريحات المالية، وغيرها من المعلومات المالية الواردة في التقرير، تُظهر بصورة عادلة ومن جميع النواحي الجوهرية الحالة المالية ونتائج العمليات لمحرر الأوراق التجارية وفقاً للفترات الزمنية المعروضة في التقرير.

(٤) المسؤولون عن التوقيع:

(أ) مسؤولون عن تأسيس وحفظ الضوابط الداخلية.

(ب) يقومون بتصميم تلك الضوابط الداخلية لضمان أن المعلومات الجوهرية المتعلقة بمُحرر الأوراق التجارية وشركاته الفرعية تكون معروفة لدى هؤلاء المسؤولين بواسطة المسؤولين الآخرين في تلك الكيانات، لاسيما خلال الفترة التي يجري فيها اعداد التقارير.

(ج) يقومون بتقييم فاعلية الضوابط الداخلية لمحرر الأوراق التجارية خلال ٩٠ يوماً قبل صدور التقرير.

(د) أن يقدموا في التقرير استنتاجاتهم حول فاعلية الضوابط الداخلية اعتماداً على تقييمهم لها اعتباراً من ذلك التاريخ.

...

مستند (١٤-٢) | مقتطفات من قسم ٩٠٦ من قانون ساربينز أوكسلي

قسم ٩٠٦. مسؤولية الشركات عن التقارير المالية.

...

''(ج) عقوبات جنائية:

'' (١) مَن يقدم أي تصريح كما هو منصوص عليه في الفقرتين (أ) و(ب) من هذ القســم مع علمه بأن التقرير الدوري المصاحب للتصريح لا ينسجم مع جميع الشروط المنصوص عليها في هذا القسم يُعاقب بغرامة لا تزيد على ١,٠٠٠,٠٠٠ دولار أو السجن مدة لا تزيد على ١٠ سنوات، أو بكليهما معاً، أو

'' (٢) مَن يقدم عمداً أي تصريح كما هو منصوص عليه في الفقرتين (أ) و(ب) من هذا القسم مع علمه بأن التقرير الدوري المصاحب للتصريح لا ينســجم مع جميع الشــروط المنصوص عليها في هذا القسم يُعاقب بغرامة لا تزيد على ٥,٠٠٠,٠٠٠ دولار أو السجن مدة لا تزيد على ٢٠ سنة، أو بكليهما معاً. ''.

مستند (١٤-٣) | قسم ٤٠٤ من قانون ساربينز أوكسلي

قسم ٤٠٤. تقييم إدارة الرقابة الداخلية.

(أ) التنظيمــات المطلوبــة: تقــوم الهيئة بكتابة التنظيمــات المفروضة على كل تقرير ســنوي والمطلوبة بموجب المادة (١٣أ) أو (١٥د) من قانون الأوراق المالية لعام ١٩٣٤ رقم (U.S.C. 15 78m, 78o (d)) لاحتواء تقرير رقابة داخلي يقوم بما يلي:

(١) توضيح مســؤولية الإدارة في إنشــاء إجراءات وهيكلة الرقابة الداخلية والحفاظ عليها وذلك لإعداد التقارير المالية.

(٢) تتضمن تقييم لفاعلية إجراءات وهيكلة الرقابة الداخلية لمحرر الأوراق التجارية وذلك لإعداد التقارير المالية، كما في تقرير نهاية السنة المالية لمحرر الأوراق التجارية.

(ب) تقييم الرقابة الداخلية واعداد تقارير بذلك: فيما يتعلق بتقييم الرقابة الداخلية التي تتطلبها الفقــرة (أ)، يجب على كل شــركة محاســبية مطروحة للتداول العام، والتي تُعــد أو تُصدر تقارير مراجعي الحسابات لمحرر الأوراق التجارية، أن تشهد، وتقدم تقريراً، عن التقييم المقدم من قبلٍ إدارة محــرر الأوراق التجارية. والشــهادة المقدمة بموجب أحكام هــذا البند يجب أن تتم وفقاً لمعايير ارتباطات الشــهادة الصادرة أو المعتمدة مــن قبل مجلس الإدارة. ويجب ألا تكون هذه الشهادة موضوع ارتباط منفصل.

ومــن وجهة نظر الأعمال فإن قســم ٤٠٤ من قانون ســاربينز أوكســلي يعرض مفهوم التحقق المعتمد على المعايير للرقابة الداخلية. وقبل إجازة قانون ســاربينز أوكسلي، كانت شركات التدقيق المحاسبي تستخدم الإجراءات الخاصة بها للتحقق من أن عمليات الشركات قوية لمنع الاحتيال. لكن أحداث فقاعة الدوت كوم كشــفت أن شركات التدقيق المحاسبي يمكن إقناعها من خلال الرســوم ووعود التعاقدات المستقبلية للتنازل عن تقييماتها وإعداد التقارير المشــبوهة. ووفقاً لذلك يتطلب قانون ســاربينز أوكســلي أن يعتمد التحقق من الإجــراءات الداخلية على قواعد يتم تأسيســها من قبل الحكومــة وليس من قبل الصناعة. وقد تم عرض قســم ٤٠٤ من قانون ساربينز أوكســلي، كما تم تظليل الجزء الذي له علاقة بهدف هذا الكتاب بالخط العريض.

والنتيجة النهائية هي أنه منذ عام ٢٠٠٣ على الشركات التحقق من أن ضوابطها الداخلية تتوافق مع المعايير التي وضعها قانون ساربينز أوكسلي. ونستعرض فيما يلي وفيما تبقى من هذا القسم نظرة عامة ذات مستوى عالي على المعايير والإجراءات المرتبطة بهذا القانون.

مجلس المراقبة المحاسبية للشركات العامة (PCAOB) ومعايير تدقيق الحسابات:

أدى إصدار قانون ســاربينز أوكســلي إلى إنشــاء هيئة باســم مجلس المراقبة المحاسبية للــشركات العامــة (Public Company Accounting Oversight Board) أو اختصــاراً (PCAOB). وفيما يلي نص من الموقع الإلكتروني لهذه المنظمة[١٦]:

مجلس المراقبة المحاســبية للشركات العامة (PCAOB) هي منظمة غير ربحية أنشأها المجلــس التشريعي للإشراف على (مراجعة حســابات الشركات العامة والوســطاء والتجار بهدف حماية المســتثمر). ويتطلب قانون ســاربينز أوكســلي لعام ٢٠٠٢، والذي أدى إلى إنشاء (PCAOB)، أن يخضع مدققو حسابات الشركات العامة في الولايات المتحدة لإشراف خارجــي ومســتقل، وذلك للمرة الأولى في التاريخ. ففي الســابق كانــت هذه المهنة ذاتية التنظيم. ويتم تعيين خمســة أعضاء في مجلس المراقبة المحاســبية للشركات العامة، بما في ذلك الرئيس، بشكل متناوب لمدة خمس سنوات، وذلك من قبل لجنة سوق المال الأمريكية (Securities and Exchange Commission) بعد التشــاور مع مجلس محافظي النظام

(16) http://pcaobus.org

الاحتياطي الاتحادي (Board of Governors of the Federal Reserve System) ووزير الخزانــة الأمريكية (Secretary of the Treasury). وتُشرف لجنة ســوق المال الأمريكية (SEC) عــلى ســلطة مجلس (PCAOB) بما في ذلك الموافقة عــلى لوائح المجلس ومعاييره وميزانيته. كما أســس قانون ساربينز أوكسلي تمويل أنشطة مجلس (PCAOB) من خلال الرسوم السنوية المقررة على الشركات العامة بما يتناسب مع قيمتها المالية، والرسوم المقررة على الوسطاء والتجار على أساس صافي رؤوس أموالهم.

وقد أصدر مجلس (PCAOB) معايير لجميع جوانب التدقيق المحاســبي(١٧). والمعايير ذات الأهمية الكبرى لنا هي معايير (AS ٥): «تدقيق الرقابة الداخلية على التقارير المالية المُدمجة مع تدقيــق البيانات المالية» ومعايير (AS 12)-»تحديــد وتقييم مخاطر الأخطاء المادية». وتوجه معايير (AS 5) الارتباطات العامة لقانون ســاربينز أوكســلي، ومن المرجح أن تكــون جزءاً من هــذه الارتباطات في حال انضمامك للعمــل في إحدى شركات التدقيق المحاســبي. وضمــن التدقيق وفقاً لقانون ســاربينز أوكســلي فإن معايــير (AS 12) تقدم إرشادات لتقنية المعلومات.

ويحدد القســم رقم ٢١ من معيار (AS 5) الاتجاه العام للتدقيق وفقاً لقانون ســاربينز أوكسلي على النحو التالي:

٢١. يجب أن يســتخدم المُدقق منهج شــمولي لتدقيق الرقابــة الداخلية على التقارير الماليــة، وذلــك لتحديد ضوابط الاختبار. ويبدأ «منهج من أعلى إلى أســفل» من مســتوى القوائــم المالية ومن فهم المدقق للمخاطر العامة للرقابة الداخلية على التقارير المالية. ثم يركز المُدقق على ضوابط مســتويات الوحدات ويعمل وصولاً إلى الحســابات والإفصاحات ذات الأهمية وتأكيداتها ذات العلاقة.

ويوجه القسم رقم ٣٦ من معيار (AS 5) المراجعين الماليين إلى الفقرة رقم ٢٩ وإلى ملحق (ب) من معيار (AS 12) وذلك للتعامل مع آثار التكنولوجيا على عملية التدقيق المالي:

٣٦. على المدقق المالي فهم كيف تؤثر التكنولوجيا على تدفق المعاملات التجارية للشركة. وعــلى المدقق المــالي تطبيق الفقرة رقم ٢٩ والملحق (ب) من معيــار التدقيق (Auditing

(17) http://pcaobus.org/Standards/Auditing/Pages/default.aspx

Standard No. 12)، وهــو معيار «تحديد وتقييــم مخاطر تحريف المواد» والذي يناقش تأثير تقنية المعلومات على الرقابة الداخلية المتعلقة بالتقارير المالية ومخاطر التقييم.

ويوجه قســم ٢٩ من معيار (AS 12) المدقق المالي بشــكل أســاسي إلى ملحق (ب) من المعيار:

٢٩. على المدقق المالي فهم كيف تؤثر التكنولوجيا على تدفق الصفقات التجارية للشركة (انظر الملحق ب).

وأخيراً فإن الملحق (ب) من معيار (AS 12) يتضمن ما يلي:

الملحق (ب): نقاط هامة بخصوص الأنظمة والضوابط اليدوية والآلية

...

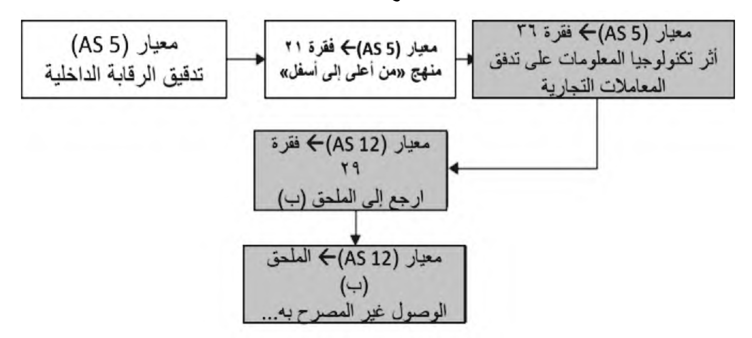
عــلى المُدقق أن يكون مدركاً للمخاطر المرتبطة بالرقابــة الداخلية للشركة على التقارير المالية والناتجة عن تقنية المعلومات. ومن الأمثلة على هذه المخاطر ما يلي:

- الاعتماد على الأنظمة أو البرامج التي تعالج البيانات بشكل غير دقيق، أو التي تعالج بيانات غير دقيقة، أو كليهما.
- الوصــول غير المصرح به للبيانات والذي قد يؤدي إلى تدمير البيانات أو إلى تغييرات غير ملائمة للبيانات بما في ذلك تســجيل معاملات غير مصرح بها أو غير موجودة أو غير دقيقة (مخاطر معينة قد تنشــأ عند وصول بعض المســتخدمين لقاعدة بيانات مشتركة).
- إمكانيــة حصول موظفي تقنية المعلومات على امتيــازات وصول تتجاوز الامتيازات اللازمة لأداء الواجبات المنوطة بهم، مما يؤدي إلى تعطيل فصل المسؤوليات.
- تغييرات غير مصرح بها لبيانات في الملفات الرئيسية.
- تغييرات غير مصرح بها على الأنظمة أو البرامج.
- فشل إجراء التغييرات اللازمة على الأنظمة أو البرامج.

- التدخل اليدوي غير الملائم.
- إمكانية فقد البيانات أو عدم القدرة على الوصول للبيانات كما هو مطلوب.

ولتسـهيل الموضوع، يوضح الشـكل (١٤-٤) المبادئ التوجيهية المذكورة أعلاه والمرتبطة بالتدقيق على تقنية المعلومات وكيفية انتقال معايير التدقيق من قسم إلى آخر.

الشكل (١٤-٤): المبادئ التوجيهية للتدقيق والتابعة لقانون (ساربينز أوكسلي) والمؤثرة في تقنية المعلومات



الرقابة الداخلية:

مـا الهـدف النهائي لجميع الأنشـطة المرتبطـة بقانون سـاربينز أوكسـلي؟ المصطلح المسـتخدم هـو «الرقابة الداخلية عـلى التقارير المالية». ويعرف هـذا المصطلح من قبل مجلس (PCAOB) في ملحق (أ) من معيار (AS 5) كما يلي:

الرقابة الداخلية على التقارير المالية عملية مصممة بواسـطة، أو تحت إشراف، الرئيس التنفيذي للشركة والمسـؤول المالي الرئيسي، أو بواسـطة أشـخاص يـؤدون وظائف مماثلة، وتُطبق من مجلس إدارة الشركـة، والإدارة وغيرهم من الموظفين، لتقديم ضمانات معقولة بشـأن مصداقيـة التقارير المالية وإعـداد القوائم المالية لأغراض خارجيـة وفقاً لـ «مبادئ المحاسبة المقبولة عموماً» (GAAP) وتشمل السياسات والإجراءات التي:

(١) تتعلـق بالمحافظة على السـجلات والتي تحتوي على التفاصيـل المطلوبة وتعرض المعاملات وترتيب الأصول في الشركة بدقة وإنصاف.

(٢) تقديم تأكيد مقبول بأن يتم تسجيل المعاملات عند الضرورة للسماح بإعداد القوائم المالية وفقاً للمبادئ المحاسبية المقبولة، وأن تتم إيرادات ونفقات الشركة وفقاً لتراخيص الإدارة ومدُيري الشركة.

(٣) تقديم ضمانات مقبولة بشأن منع الاستحواذ غير المصرح به أو كشف ذلك في التوقيت المناسب، وكذلك بشأن الاستخدام غير المصرح به لأصول المنظمة التي يمكن أن يكون لها تأثير جوهري في البيانات المالية.

وتُعد الرقابة الداخلية على التقارير المالية مجموعة فرعية من أنشطة الرقابة الشاملة في الشركة. وفي مجال قانون ساربينز أوكسلي، يمكن تعريف أنشطة الرقابة بأنها الإجراءات والأساليب والسياسات التي يستخدمها الشخص المسؤول لتقليل احتمال وقوع الأحداث المحفوفة بالمخاطر إلى مستويات مقبولة. وهذا التعريف ينسجم مع تعريف ضوابط تكنولوجيا أمن المعلومات الذي استخدمناه في هذا الكتاب، وهو إجراءات الحماية المستخدمة لتقليل أثر التهديدات.

الضوابط العامة لتقنية المعلومات:

الجزء الأكبر من أنشطة مراجعة الرقابة الداخلية يتم تنفيذه بواسطة مدققي الحسابات والمحاسبين. لكن هؤلاء المتخصصين يعتمدون على خبراء تقنية المعلومات للمساعدة في تقييم الضوابط الموضحة في ملحق (ب) من معيار (AS 12). وتقليدياً، تُسمى هذه الأنشطة بالضوابط العامة لتقنية المعلومات.

ولا يبدو أن الإصدارات الحالية لمعايير التدقيق المحاسبي تحتوي على تعريف لمصطلح «الضوابط العامة لتقنية المعلومات». لكن معيار (AS 2)، والذي حل محل معيار (AS 5)، مدرج في الفقرة رقم ٥٠[١٨]:

بعض الضوابط (مثل الضوابط التي على مستوى الشركة والموضحة في فقرة ٥٣) قد يكون لها تأثير متزايد في تحقيق الأهداف العامة لمعايير الرقابة. على سبيل المثال، الضوابط العامة لتقنية المعلومات على تطوير البرامج وتغييرها، وعمليات الحاسب الآلي، والوصول

(18) http://pcaobus.org/standards/auditing/pages/auditing_standard_2.aspx

إلى البرامــج والبيانات تُســاعد في التأكد من أن الضوابط المحددة عــلى معالجة المعاملات تعمل بشــكل فعال. وفي المقابل فإنه يتم تصميــم ضوابط أخرى لتحقيق أهداف محددة لمعايير الرقابة. على ســبيل المثال، تحدد الإدارة عادة ضوابط محددة مثل المحاسبة لجميع وثائق الشحن، لضمان تسجيل جميع المبيعات الصحيحة.

وفي حين أن معيار (AS 2) يقدم مثالاً فقط ولم يقدم تعريف رســمي للضوابط العامة لتقنيــة المعلومات، إلا أن فقرة ٥٠ تشــير إلى تعريف لهذا المصطلح. واســتناداً إلى الفقرة ٥٠ مــن معيــار (AS 2)، يمكن مقارنة الضوابط العامــة بالضوابط الخاصة من حيث تقدم الضوابط العامة المنصة الأساســية لإنجاز العديد من الضوابط المحددة. على ســبيل المثال، إذا كان نظام تقنية المعلومات يســمح للمســتخدم أن يســجل المعاملات دون كلمة مرور، فإن احتمال المعاملات الاحتيالية يزداد بشــكل كبير مما يضعــف فاعلية الضوابط الخاصة المصممة للتحقق من الأنشطة التجارية المختلفة. لذلك يعد الحفاظ على بنية تحتية آمنة لتقنية المعلومات من خلال الضوابط العامة أمر مهم للتحقق بشــكل موثوق من الأنشطة التجارية. وبناء على هذا نُعرف الضوابط العامة لتقنية المعلومات بأنها أنشطة الرقابة التي تقــوم بها تقنية المعلومات والتي تضمن المعالجة الصحيحــة للمعاملات التجارية من قبل المنظمة.

وعند المشاركة المتعلقة بقانون ساربينز أوكسلي فإن خبراء تقنية المعلومات يشاركون في تدقيق الضوابط العامة لتقنية المعلومات.

إجــراءات التحقق من الضوابــط العامة لتقنية المعلومات كجزء مــن التدقيق المتعلق بقانون ساربينز أوكسلي:

وفقاً لمبدأ التوجيه «من أعلى إلى أسفل» والتابع لمعيار (AS 5)، فإن الصناعة قد وضعت الإجراءات التالية لتدقيق الضوابط العامة لتقنية المعلومات على التقارير المالية[١٩].

١. النظر في التقارير المالية للمنظمة.

٢. تحديد بنود المواد:

(١٩) ولمزيــد مــن التفاصيــل انظــر الرابــط التــالي: http://www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/IT-Control-Objectives-for-Sarbanes-Oxley (accessed 1/1/2013)

٣. ما يحتاج المستثمر المتعقل أن يعرفه.

٤. تحديد العمليات التجارية التي تصب في هذه البنود.

٥. تحديد منصات تقنية المعلومات التي تدعم هذه العمليات-نظم التشـغيل، قواعد البيانات، التطبيقات، خوادم الشبكات.

٦. التأكد من تحقيق أهداف الضوابط العامة لتقنية المعلومات والمرتبطة بتلك المنصات.

٧. إعداد تقرير بنقاط ضعف المواد.

الخلـل الذي قد يؤدي إلى حدوث تحريـف في التقارير أو أن يظل ذلك التحريف دون اكتشاف.

وهذه العملية تتكرر سنوياً وذلك للامتثال لقانون ساربينز أوكسلي. وللعنصر رقم ٥ في القائمة أعلاه، تم تحديد ١٢ هدفاً رقابياً اعتماداً على أفضل ممارسات الصناعة، متضمناً ذلك بنود مثل إدارة التغيير وإدارة البيانات[٢٠].

الامتثال في مقابل إدارة المخاطر:

المثال المتعلق بقانون سـاربينز أوكسلي في مجال الضوابط العامة لتقنية المعلومات على التقاريـر الماليـة والذي تم عرضه في الجزء السـابق يدل على أن الكثير من أنشـطة إدارة المخاطر يتم فرضها بواسـطة القانون واللوائح. وفيما سـبق عرفنا الامتثال بأنه نشاط اتباع القوانين واللوائح والأنظمـة والالتزامات التعاقدية ذات العلاقة. وإذا كان الجزء الأكبر من إدارة المخاطر يتم تحديده بواسـطة القوانين واللوائح، قد تتساءل لماذا تبذل المنظمة جهداً في تطوير خطة إدارة مخاطر خاصة بها اعتماداً على معايير (NIST 800 -39) أو على معايير (ISO 27000). لماذا لا يتم تعهيد إدارة المخاطر للمشرعين وخبراء الصناعة، وتقوم المنظمة بالامتثال للقوانين واللوائح ورموز الصناعة وغيرها والتي يطورها هؤلاء الخبراء؟

وإذا فكرت في هذا التسـاؤل سوف تدرك أن الامتثال ليس إلا مجموعة جزئية من إدارة المخاطر، ومن ثم فإن الامتثال يتطلب مجموعة صغيرة من أنشطة إدارة المخاطر لمنع وقوع

(٢٠) انظر شكل (١) في صفحة ١١ من الوثيقة الموجودة في رابط الهامش السابق.

الكوارث التي يمكن أن تؤثر في الآخرين. الامتثال لا ينظم المخاطر التي تؤثر فقط فيك وفي منظمتك.

على سبيل المثال، يحق للمرء أن يبدد دخله على مشتريات لا داعي لها. وطالما أن النتائج السلبية لهذه الأنشطة محدودة بالشخص وحده، فلا يوجد أي لوائح أو قوانين تمنع الشخص من القيام بتلك الأنشطة. لكن عند قيادة السيارة على الطريق، فإن سلوك الفرد الخطر قد يضع السائقين الآخرين في خطر. لذا يُطلب من السائقين الالتزام بقوانين القيادة الآمنة، كما تُفرض عقوبات صارمة للقيادة تحت تأثير الكحول.

وبالمثل فإن أنشطة الامتثال التابعة لإدارة مخاطر تقنية المعلومات تضمن أن سلوك المنظمة لا يضع المستثمرين والمنظمات الأخرى في خطر. لكنك وحدك المسؤول عن التأكد من أن أنشطتك لا تضع منظمتك الخاصة في خطر. وإدارة المخاطر تغطي كل ما عليك فعله حتى لا تضر نفسك.

الترويج للأمن:

ليس من السهل الترويج لأمن تقنية المعلومات. فالإدارة العليا عادة ما تفكر في «العائد على الاستثمار» (Return on Investments)، ومن الصعب في كثير من الأحيان قياس العائد على شيء «قد» يحدث مثل انقطاع التيار الكهربائي أو حوادث القرصنة. وعلى الرغم من سهولة تبرير التكاليف اعتماداً على الحوادث المعروفة والحالية، ما زالت بعض المنظمات مترددة في تحصيص موارد للأمن.

وأحد أفضل الإستراتيجيات هي محاولة تحديد نسبة معينة لإنفاقها في مجال الأمن في كل مشروع من مشاريع تقنية المعلومات. على سبيل المثال، المشروع الذي يتضمن «إدارة الهوية والوصول» (Identity and Access Management) قد يتضمن أيضاً تكلفة البرمجيات اللازمة لتشفير البيانات الشخصية مثل أرقام الضمان الاجتماعي (Social Security Numbers). وإذا تم التفاوض على اتفاقية البرمجيات بالشكل الصحيح، فإنه يمكن ترخيص نفس البرمجيات لتشمل أيضاً إذن تشفير البيانات المقيدة الأخرى في بقية الخوادم.

وللأسف فإن واحدة من أسهل الطرق للحصول على التمويل هي الاستفادة من الحوادث التي وقعت للمنظمات المشابهة. مثلاً تسرب أرقام الضمان الاجتماعي في الجامعات القريبة سيثير دون أدنى شك تساؤلات حول الأمن الداخلي في جامعتك. الطلاب سيتساءلون عن كيفية حماية أرقام الضمان الاجتماعي، وقد تتساءل وسائل الإعلام المحلية عن ذلك أيضاً. وخلال هذه الأوقات، قد تحصل إدارة تقنية المعلومات على تمويل كبير لتحسين الموقف الأمني للبنية التحتية. ومن المهم أن يكون هناك إستراتيجية جاهزة للاستفادة من هذه الحالات وألا يتم تبديد تلك الأموال في شراء موارد لا حاجة لها.

نموذج حالة - الشراء من أسواق الإنترنت:

في الخامس من ديسمبر من عام ٢٠١٢، أعلن المدعي العام الأمريكي للمقاطعة الشرقية من مدينة نيويورك اعتقال ستة أشخاص رومانيين وواحد ألباني بتهمة الاحتيال على الزبائن الأمريكيين، وذلك في أسواق الإنترنت المشهورة مثل (eBay)، و(AutoTrader.com)، و(Cars.com). وتم الاعتقال بتعاون وكالات إنفاذ القانون في رومانيا، وجمهورية التشيك، والمملكة المتحدة، وكندا، والولايات المتحدة الأمريكية.

نشر المحتالون إعلانات تفصيلية لسلع باهظة الثمن كالسيارات والقوارب في أسواق الإنترنت المشهورة، على الرغم من أن تلك السلع لم تكن موجودة في الواقع. واستعان المحتالون بمتآمرين مشتركين معهم والذين يُسمون بـ «السهام» في الولايات المتحدة لفتح حسابات مصرفية باستخدام جوازات سفر مزورة بطريقة عالية الجودة. وقد استجابت تلك السهام لطلبات الزبائن المرتقبين، وحصلوا في مقابل ذلك على الأموال.

وتم تحويل المدفوعات من الضحايا المطمئنين إلى خارج الولايات المتحدة بواسطة السهام إما نقداً أو عن طريق الحوالة البنكية. وفي إحدى الحالات تم إرسال ١٨ ألف دولار إلى خارج الولايات المتحدة بداخل مكبرات صوت. وفي حالة أخرى تم استخدام الأموال لشراء ساعات باهظة الثمن ومن ثم إرسالها عبر البريد إلى المحتالين. وبلغ مجموع الأرباح المقدرة لهذه العصابة ٣ ملايين دولار.

المرجع:

https://www.justice.gov/usao/nye/pr/2012/2012dec05.html

الملخص:

في هــذا الفصل اســتعرضنا تحليــل المخاطر والنــماذج المتاحة لتحليــل المخاطر. كما استخدمنا تحليل المخاطر لربط محتويات هذا الكتاب بالأهداف الإدارية الشاملة للمنظمة. ومن خلال نموذج (NIST 800 -39) لتحليل المخاطر، اســتعرضنا جميع المعلومات الواردة في الأجزاء الســابقة من هذا الكتاب بشــكل يتفق مع المعايير الموصى بها لتحليل المخاطر. كــما رأينا أن تحليــل المخاطر يربط كل تهديد بجميع نتائجه الممكنة مما يقدم آلية لقياس المخاطر وذلك بهدف المقارنة والتقييم. وناقشنا أيضاً نموذج محدد لإدارة المخاطر والمتعلق بقانون ساربينز أوكسلي والذي يستخدم من قبل الشركات المطروحة للتداول العام لطمأنة المستثمرين بمصداقية التقارير المالية.

أسئلة مراجعة للفصل:

١. ما المخاطر؟ وفي رأيك، ما أهم ثلاث مخاطر لتقنية المعلومات واجهتها شخصياً؟

٢. ما إدارة المخاطر؟ اذكر نشــاطاً أو نشــاطين يمكنك القيام بها لجعل المخاطر التي حددتها في السؤال الأول يُمكن التنبؤ بها.

٣. اذكر نشــاطاً أو نشاطين يمكنك القيام بها للاســتعداد ولتقليل المخاطر التي حددتها في السؤال الأول.

٤. ما النماذج؟ ولماذا تستخدم في الإدارة؟ صف باختصار (في جملة واحدة إلى جملتين) نموذجاً درســته في مادة أخرى. وضح كيف أن استخدام النموذج يساعدك على فهم الموضوع المنظم بواسطة النموذج.

٥. ما أهداف نموذج (NIST 800 -39)؟

٦. مــا أنواع المخاطر التنظيميــة المذكورة في نموذج (NIST 800 -39) (صفحة ١، فقرة ٢ من المعيار)؟

٧. انظر في التقرير الشامل للأداء (10-K) المُقدم من قبل شركة (Apple Computer) (أو إذا كنــت تفضل أي شركة كــبرى في مجال تقنية المعلومات ومطروحة للتداول

العـــام مثـــل (HP)، (IBM)، (Dell)، (Oracle)، (Microsoft)). اذكـــر جميـــع المخاطر المحددة بواســـطة الشركة عـــلى أنها عوامل مخاطـــر (ولخص كل منها في عبارة قصيرة). صنف تلك العوامل بأنها أحد المخاطر التنظيمية المذكورة في نموذج (NIST 800 -39).

٨. قـــدم لمحة عامة عن نموذج إدارة المخاطر (NIST 800 -39). ارســـم شـــكلاً يوضح عناصر النموذج وعلاقة هذه العناصر فيما بينها.

٩. مـــا إدارة مخاطـــر تقنية المعلومات؟ ما العلاقة بـــين إدارة مخاطر تقنية المعلومات وإدارة المخاطر الشاملة للمنظمة؟

١٠.مـــا إطار المخاطر كما ورد في نمـــوذج (NIST 800- 39)؟ وما دور إطار المخاطر في إدارة مخاطر تقنية المعلومات؟

١١. مـــا تقييم مخاطر تقنية المعلومات كما ورد في نموذج (NIST 800 -39)؟ وما دور تقييم مخاطر تقنية المعلومات في إدارة مخاطر تقنية المعلومات؟

١٢.ما الاستجابة لمخاطر تقنية المعلومات كما وردت في نموذج (NIST 800- 39)؟ وما دور الاستجابة لمخاطر تقنية المعلومات في إدارة مخاطر تقنية المعلومات؟

١٣.ما رقابة مخاطر تقنية المعلومات كما وردت في نموذج (NIST 800- 39)؟ وما دور رقابة مخاطر تقنية المعلومات في إدارة مخاطر تقنية المعلومات؟

١٤.ما العلاقة بين المخاطر والتهديدات؟

١٥.أثناء مرحلة تحديد المخاطر كمرحلة من مراحل تقييم المخاطر، ما البنود التي يجب معرفتها لتحديد المخاطر؟

١٦.اكتب المخاطر التي حددتها في السؤال الأول على شكل عبارات مخاطر وذلك باتباع الأمثلة الموجودة في هذا الفصل. وحدد بوضوح جميع عناصر المخاطر في كل عبارة من عبارات المخاطر.

١٧.لكل خطر من المخاطر المحددة في سؤال ١٦، واعتماداً على رأيك، قدّر احتمال وتأثير

كل خطر. وباستخدام هذه التقديرات، قم بقياس كل خطر من تلك المخاطر ورتبها استناداً إلى تلك التقديرات.

١٨.قدم لمحة موجزة عن سلسلة معايير (ISO 27000) والتي وضعتها المنظمة الدولية للمعايير (ISO). وما العلاقة بينها وبين معايير (NIST 800- 39)؟ وإذا كان عليك اختيار واحد من هذين المعيارين، فأي معيار ستختار كمعيارك المرجعي لإدارة مخاطر تقنية المعلومات؟ ولماذا؟

١٩.قدم لمحة موجزة عن منهجية (OCTAVE) والتي وُضعت بواسطة معهد هندسة البرمجيات (SEI). ما العلاقة بين هذه المنهجية من جهة وبين معيار (NIST 800-39) ومعيار (ISO 27000) من جهة أخرى؟

٢٠.ما هي بعض الأحكام المهمة التي حددها قانون ساربينز أوكسلي؟

٢١.ما هي بعض الاختلافات الهامة بين الأحكام في أقسام (٣٠٢) و (٤٠٤) من قانون ساربينز أوكسلي؟

٢٢.ما الرقابة الداخلية كما تم تعريفها في قانون ساربينز أوكسلي؟

٢٣.ما معايير التدقيق المحاسبي؟

٢٤.اشرح باختصار إجراءات التدقيق المحاسبي التي تتم «من أعلى إلى أسفل» وذلك للتحقق من الضوابط العامة لتقنية المعلومات كجزء من مراجعة قانون ساربينز أوكسلي.

٢٥.ما الفرق بين إدارة المخاطر والامتثال؟

أسئلة على نموذج الحالة:

١. اقرأ إعلان مكتب المدعي العام من خلال الرابط الموجود في هذه الحالة. واذكر ما تعرفه من الآليات التي يستخدمها المحتالون لإقناع العميل المُرتقب بصحة إعلاناتهم التجارية.

٢. بنـــاءً على هذه الحادثة، مـــا الاحتياطات التي تنصح بها صديقك الذي يفكر في شراء سلعة باهظة الثمن من الإنترنت؟

نشاط التدريب العملي - تقييم المخاطر باستخدام الأمر (lsof):

في هذا النشـــاط، ســـوف تتعلم اســـتخدام الأمر (lsof) لمراجعة الأوامر المستخدمة في اتصال الشبكة ولإجراء تقييم المخاطر لآلة لينكس الافتراضية.

وللبدء، انتقل إلى الحســـاب ذو الامتيازات العالية، وقم بتشـــغيل الأمر (lsof -i) وذلك لمشاهدة جميع اتصالات الشبكة المفتوحة:

```
[alice@sunshine   ]$ su -
Password:  thisisasecret

[root@sunshine   ]# lsof -i
COMMAND    PID    USER  FD TYPE   DEVICE SIZE/OFF NODE NAME
sshd      1862    root  3u IPv4    11083      0t0 TCP *:ssh (LISTEN)
sshd      1862    root  4u IPv6    11085      0t0 TCP *:ssh (LISTEN)
ntpd      1870     ntp 16u IPv4    11113      0t0 UDP *:ntp
ntpd      1870     ntp 17u IPv6    11114      0t0 UDP *:ntp
ntpd      1870     ntp 18u IPv6    11118      0t0 UDP v6.sunshine.edu:ntp
ntpd      1870     ntp 19u IPv6    11119      0t0 UDP [fe80::a00:27ff:fef6:cadf]:ntp
ntpd      1870     ntp 20u IPv4    11120      0t0 UDP sunshine.edu:ntp
ntpd      1870     ntp 21u IPv4  1878265      0t0 UDP 10.0.2.15:ntp
mysqld    2148   mysql 10u IPv4    11438      0t0 TCP *:mysql (LISTEN)
master    2276    root 12u IPv4    11742      0t0 TCP sunshine.edu:smtp (LISTEN)
master    2276    root 13u IPv6    11744      0t0 TCP v6.sunshine.edu:smtp (LISTEN)
httpd     2316    root  4u IPv6    11985      0t0 TCP *:http (LISTEN)
qpidd     2335   qpidd 10u IPv4    12079      0t0 TCP *:amqp (LISTEN)
qpidd     2335   qpidd 11u IPv6    12080      0t0 TCP *:amqp (LISTEN)
dnsmasq   13558 nobody  4u IPv4  1877904      0t0 UDP *:domain
dnsmasq   13558 nobody  5u IPv4  1877905      0t0 TCP *:domain (LISTEN)
dnsmasq   13558 nobody  6u IPv6  1877906      0t0 UDP *:domain
dnsmasq   13558 nobody  7u IPv6  1877907      0t0 TCP *:domain (LISTEN)
dhclient  13624   root  6u IPv4  1878166      0t0 UDP *:bootpc
httpd     31152 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31153 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31154 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31156 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31157 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31158 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31159 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
httpd     31160 apache  4u IPv6    11985      0t0 TCP *:http (LISTEN)
```

وتقدم لك مخرجات هــذا الأمر معلومات مهمة عن البرمجيات التي تعمل على النظام مثل:

- اسم البرنامج الذي يعمل (COMMAND).
- المستخدم الذي يشغل البرنامج (USER).
- رقم عملية البرنامج (PID).
- المنفذ الذي يتصل به البرنامج أو ينتظر عملية الاتصال (NAME).

وأكثر هذه الأعمدة أهمية هو عمود (NAME). ويكون شــكل المُدخلات على الشكل التالي:

server: port (STATE):

بحيث يكون الخادم هو جهاز الحاسب الآلي (اسم الجهاز أو عنوان بروتوكول الإنترنت)، والعملية تكون متصلة به، والمنفذ هو اسم الخدمة التي تستخدمها العملية. أما رقم المنفذ المتصلة به العملية فيتحول إلى اسم خدمة من خلال البحث عنه في دليل (/etc/services). ولأن أرقام المنافذ يمكن اســتخدامها في خدمــات متعددة، فإن هذا البحث ليس موثوق به دائماً لكنه يساعد على التخمين الجيد.

وقوائــم الاتصال التي تبدأ بعلامــة النجمة (*) لا تكون متصلة بخــادم خارجي. هذه القوائم تســتمع لاتصال معين، ومن ثم فإن حالة الاستماع (LISTEN) تكون مضافة لكثير من هذه المُدخلات.

قم بالبحث في الإنترنت عن مزيد من المعلومات حول كل عملية من العمليات المدرجة في مخرجات أمر (lsof) وقم بتجميع المعلومات في جدول.

مثال:

متصل بمضيف آخر	تستمع لاتصال	رقم المنفذ	الوصف	العملية
نعم	نعم	123	بروتوكول وقت الشبكة (Network Time Protocol)- هذه الخدمة تعمل على تزامن وقت النظام مع وقت خوادم الشبكة	ntpd

أسئلة:

١. في رأيك، ما الخدمات (إن وجدت) التي يمكن أن تمثل خطراً على الأمن وقد تحتاج إلى تعطيل؟

٢. بدلاً من تعطيل الخدمة، ما الضوابط الأخرى التي يمكن وضعها للتقليل من المخاطر؟

تمرين التفكير النقدي-تقديرات المخاطر المتحيزة:

في السنوات الأخيرة، كان هناك الكثير من الأبحاث حول كيفية تحيز الأشخاص في تقييم المخاطر. ويقول كاس سنشتاين (Cass Sunstein)، وهو أحد أبرز الباحثين القانونيين في عصرنا، «الثقافات المتنوعة تركز على مخاطر مختلفة جداً، مع الضغوط الاجتماعية وضغوط الأقران التي تُبرز بعض المخاوف وتقلل من مخاوف أخرى. الاندفاعات، وتوفر الحدس المهني، وفقد الكراهية، واستقطاب المجموعة، كلها أمور ذات أهمية هنا». وفي مقال في صحيفة نيويورك تايمز، وصف البروفسور جاريد دياموند (Jared Diamond) كيف يتجاهل الناس المخاطر عندما يكون احتمال حدوثها في كل فرصة منخفض، حتى لو كان هناك تكرار كبير جداً لتلك الفرص مثل قيادة السيارة. وفي مجال بحثي متصل يُسمى بـ «الإدراك الثقافي»، يقول البروفسور دان كاهان (Dan Kahan) من جامعة ييل (Yale University) «الثقافة تسبق الحقائق» وذلك أن الناس يقبلون بشكل انتقائي ويرفضون الحقائق بالطريقة التي تدعم وجهات نظرهم.

المراجع:

Sunstein, C.R. «Laws of Fear: Beyond the Precautionary Principle,» Cambridge University Press, March 2005. Available at SSRN: http://ssrn.com/abstract = 721562

Diamond, J. «That daily shower can be a killer,» New York Times, 012013/28/

Schneier, B. Cryptogram, February 1, 2013

Kahan, D.M., Slovic, P., Braman, D., and Gastil, J. «Fear of democracy: A cultural evaluation of Sunstein on risk,» Harvard Law Review, 2006, 119, Yale Law School, Public Law Working Paper No. 100, Yale Law & Economics Research Paper No. 317. Available at SSRN: http://ssrn.com/abstract = 801964

أسئلة على تمرين التفكير النقدي:

١. خــلال تقييم مخاطر تقنية المعلومــات، ما هي بعض الطرق التي يؤدي فيها التحيز في التقدير إلى المبالغة في تقدير المخاطر غير المهمة، والتقليل من المخاطر المهمة؟

٢. يشــار إلى أن المبالغة في تقدير المخاطر تؤدي بالضرورة إلى عدم التقدير التام لبعض المخاطر الهامة. هل تتفق مع هذا التقييم؟ علل إجابتك.

تصميم حالة:

الآن وبعد أن انتهيت من هذا المقرر الدراسي، حان الوقت أن نقدم الخلاصة. في مثالنا أنك عملت في جامعة ولاية الشمس المشرقة لمدة عام دراسي إلى الآن، وقد طلب منك مدير الجامعة أن تضعا معاً تقييماً لمخاطر المنظمة. قم بإنشــاء تقييم مبســط للمخاطر استناداً إلى جميــع تصميــم الحالات التــي عملت عليها إلى الآن في هذا الكتــاب. وفيما يلي بعض الإرشادات:

- قــم بمراجعة وإعــادة تقييم جميع «تصميــم الحالات» في جميــع الفصول في هذا الكتاب من أجل إعداد وثيقة لتقييم المخاطر.
- اجعل وثيقة تقييم المخاطر سهلة القراءة.
- استخدم الرسوم البيانية لتوضيح النقاط.
- قارن الوضع الحالي لجامعة ولاية الشمس المشرقة بجامعات أخرى كلما أمكن ذلك.
- ابحث التحديات الممكنة التي يمكن أن تُثيرها التقنيات الجديدة.
- أنهي الوثيقة ببعض النقاط المقترحة لتحسين الحالة الأمنية للجامعة.

ملحق أ: قائمة بكلمات المرور لآلة لينكس الافتراضية

يوجد بعض الحسابات المهيئة مسبقاً لآلة لينكس الافتراضية والمستخدمة في التدريبات العملية في هذا الكتاب. ويتضمن الجدول التالي بعض الحســابات التي تم اســتخدامها في التدريبــات العملية. وللحصول على قائمة كاملة للحســابات وكلــمات المرور، افتح الدليل التالي (root/passwords.list/) في محرر نصي على الآلة الافتراضية.

اسم المستخدم	كلمة المرور
root	thisisasecret
alice	aisforapple
bob	bisforbanana
charlie	cisforcookie
dave	disfordog
eric	eisforelephant
fred	fisforfrog

المصطلحات:

- **تدقيــق الوصول (Access audit):** عملية تحديد الوصول الذي يســتحقه كل فرد بناءً على البيانات المُقدمة من سجل الشخص والسياسات الأمنية الحالية.
- **التحكم في الوصول (Access control):** هو تقييد الوصول إلى موارد نظم المعلومات للمصرح لهم فقط من المستخدمين والبرامج والعمليات والنظم.
- **نماذج التحكم في الوصول (Access control models):** توضيح لمدى توافر الموارد في النظام.
- **قائمــة التحكم في الوصــول (Access control list):** هي قائمة من الأذونات تتبع مكونات محددة.
- **نظــام إدارة الوصــول (Access management system):** جميــع السياســات، والإجراءات والتطبيقات التي تأخذ البيانات من ســجل الشــخص ونظام الســجلات بهدف اتخاذ قرار بشأن منح صلاحيات الوصول للموارد.
- **ســجل الوصول (Access registry):** الأداة التي توفر لمسؤولي الأمن رؤية موحدة لحسابات وأذونات الأفراد عبر المنظمة بأكملها.
- **النشــاط (Action):** هو العمل الذي يقوم به الوسيط للتأثير على خصوصية الأصل أو تكامله أو جاهزيته.
- **الدليل النشط (Active Directory):** هو مجموعة من التقنيات التي توفر المركزية لإدارة المستخدم وللتحكم في الوصول لكافة الأجهزة الموجودة في نفس المجال.
- **خدمــات الارتباط الاتحــادي للدليل النشــط (Active Directory Federation Services):** خدمة توســيع نظام الدليل النشــط لدعم وصــول الارتباط الاتحادي إلى الموارد المحلية والخارجية باســتخدام بروتوكول «لغــة تمييز التأكيدات الأمنية» والبروتوكولات الأخرى. ويشار لها اختصاراً (ADFS).
- **التهديد المتقدم الدائم (Advanced persistent threat):** وهو هجوم بشري متواصل ومكثف يتم من خلاله رفع المدى الكامل لتقنيات التسلل لأجهزة الحاسب الآلي.

- **أنظمة كشف التسلل المُعتمدة على الانحرافات (Anomaly-based detection):** هي عملية الكشف عن الانحرافات بين الأحداث المُلاحظة وأنماط النشاط المحددة.
- **الأصول (Asset):** هي الموارد أو المعلومات التي يجب حمايتها.
- **أهمية الأصول (Asset criticality):** هي مقياس لمدى أهمية الأصل للبقاء الحالي للمنظمة.
- **مالك الأصل (Asset owner):** هو فرد أو وحدة يملك مسؤولية تشغيلية لجميع الوظائف غير المتوقعة والمرتبطة بتأمين الأصل.
- **حساسية الأصول (Asset sensitivity):** هي مدى الضرر الذي يحدث للمنظمة بسبب اختراق خصوصية الأصول أو انتهاك تكاملها.
- **المصادقة (Authentication):** هي العملية التي يقوم فيها المستخدم بإثبات أنه المالك للهوية التي يتم استخدامها.
- **المصادقة المعتمدة على الرمز المشترك (Authentication token):** هي استخدام مُعرِف فريد أو دالة تجزئة مشفرة تُثبت هوية المستخدم بملكيته للرمز.
- **الجاهزية (Availability):** هي ضمان الوصول الموثوق للمعلومات واستخدامها في الوقت المناسب.
- **الأجهزة الحيوية (Biometric devices):** هي أجهزة تحلل الفروق الدقيقة في بعض المواصفات الجسدية أو السلوكية، مثل بصمات الأصابع أو نمط الأوعية الدموية في العين، وذلك لتحديد هوية الفرد.
- **العلامات الحيوية (Biometric markers):** هي الفروق المادية التي يمكن ملاحظتها بين الناس.
- **تشفير المجموعات (Block encryption):** هو عملية تحويل مجموعات النص العادي إلى مجموعات مشفرة.

- **هجوم القوة الغاشــمة (Brute-force attack):** هو الطريقة التي يحاول قراصنة الحاســب من خلالها الوصول إلى حســاب عــلى النظام المســتهدف وذلك بمحاولة «تخمين» كلمة المرور الصحيحة.
- **تجاوز سعة المخزن المؤقت (Buffer overflow vulnerability):** هي الحالة التي يقــوم فيها برنامج بوضع المزيد من المعلومات في مكان التخزين أكثر مما يســتطيع المخزن تحمله.
- **تحليــل تأثــير العمــل (Business impact analysis):** هــو تحديــد الخدمات والمنتجات البالغة الأهمية للمنظمة.
- **بروتوكــول خدمــة المصادقــة المركزيــة (Central Authentication Service protocol):** هــي أحد التقنيات الرائدة في «تســجيل الدخول الأحادي» المفتوحة المصدر، وخصوصاً في مجال التعليم العالي.
- **التوثيــق (Certificate):** هــو مجموعة من المعلومات تحتــوي على المفتاح العام المشفر للخادم، كما تحتوي على التعريف بمزود المفتاح.
- **أمر تغيير الدليل (cd):** هو الأمر الخاص بتغيير الدليل والذي يســمح بالتبديل إلى دليل آخر. ويتم تحديد اسم المجلد المستهدف كمعامل للأمر.
- **خاصية المجموع الاختياري (Checksum):** هو قيمة يتم حسابها بناء على البيانات بهدف كشف الأخطاء أو كشف التلاعب في البيانات أثناء الإرسال.
- **مصطلح (Ciphertext):** هو النص المشفر غير المفهوم للقارئ.
- **الحوســبة السحابية (Cloud computing):** هي تقديم البرامج وغيرها من موارد الحاسب الآلي عبر الإنترنت كخدمة وليس كمنتج منفصل.
- **الامتثــال (Compliance):** هو عملية اتباع القوانــين، والأنظمة، والقواعد، ورموز الصناعة، والالتزامات التعاقدية.
- **حــوادث أمن الحاســب الآلي (Computer security incident):** هي انتهاك أو تهديد وشيك بانتهاك سياســات أمن الحاسب الآلي، أو سياسات الاستخدام المقبول، أو ممارسات الأمان الموحدة.

- **كلــمات المــرور المخترقــة (Compromised passwords):** هــي كلــمات مرور موجودة على النظام ويعرفها مستخدمون غير مصرح لهم.
- **الخصوصية (Confidentiality):** هي الحفاظ على القيود المُرخصَة للإذن بالدخول على الأنظمة والإفصاح عن المعلومات بما في ذلك وسائل حماية الخصوصية الشخصية والمعلومات السرية.
- **الضبــط (Configuration):** هــو اختيــار مجموعــة مواصفات النظــام من بين المجموعات الممكنة.
- **الضوابط الأمنية (Controls):** هي الإجراءات الوقائية المُســتخدمة للحد من تأثير التهديدات.
- **أنشطة الرقابة (Control activities):** هي الإجراءات والأساليب والسياسات التي يســتخدمها الشخص المسؤول لتقليل احتمال وقوع الإحداث المحفوفة بالمخاطر إلى مستويات مقبولة.
- **بيانات الاعتماد (Credentials):** هي جزء (أو أجزاء) من المعلومات المُســتخدمة في التحقق من هوية المستخدم.
- **البرمجة النصية المشتركة للمواقع الإلكترونية (Cross-site scripting):** هي ثغرة تحدث عند اســتخدام المدخلات المُجهــزة من قبل المســتخدم دون إجراء التحقق باعتبارها جزء من المخرجات المُقدمة لمستخدمين آخرين.
- **تحليل الشفرات (Cryptanalysis):** هو فن كسر النص المشفر.
- **خوارزمية التشــفير (Cryptographic algorithm):** هي تسلسل من الخطوات المستخدمة والمحددة بشكل جيد لوصف عمليات التشفير.
- **الكتابة السرية للبيانات (Cryptography):** هي الفن أو العلم الذي يقوم بتسليم معلومات لا يمكن فهمها واستعادة المعلومات المشفرة في شكل مفهوم.

- **الجُدُر النارية للفحص العميق للحــزم (Deep packet inspection firewalls):** هــي أدوات تقوم بفحص البيانات التي تحملها الحزمة، بالإضافة إلى فحص الحقول العلوية لبروتوكول الحزم، وذلك لاتخاذ قرار بشأن كيفية التعامل مع الحزمة.
- **حالة السماح الافتراضي (Default allow stance):** هي حالة ضبط الجدار الناري بحيث يسمح لجميع الحزم في الشبكة باستثناء تلك المحظورة صراحة.
- **حالة الرفض الافــتراضي (Default deny stance):** هي حالة ضبط الجدار الناري بحيث يحظر جميع الحزم في الشبكة باستثناء تلك المسموح بها صراحة.
- **الأصول المؤجلة (Deferrable asset):** هي الأصول اللازمة للتشغيل المثالي للمنظمة لكن فقدان جاهزيتها لا يسبب مشكلات كبيرة للمنظمة في الأجل القريب.
- **المنطقة منزوعة الســلاح (Demilitarized zone):** انظر تعريف الشبكة المحيطة (perimeter network).
- **رفــض الخدمــة (Denial of service):** هو المنع غير المــصرح به من الوصول إلى الموارد أو تأخير العمليات الحساسة ذات الوقت الحرج.
- **التوقيعــات الرقمية (Digital signatures):** هي تحويلات مشــفرة من البيانات تسمح لمُستقبِل البيانات بإثبات مصدر البيانات (عدم التنصل) وتكاملها.
- **الكارثة (Disaster):** هي حادثة مفجعة تتسبب في دمار كبير.
- **التعافي من الكوارث (Disaster recovery):** هي العملية التي تقوم بها منظمة تقنية المعلومات من أجل إعادة الأنظمة الاحتياطية وتشغيلها. ويشار إليها اختصاراً (DR).
- **خدمــة الاكتشــاف (Discovery service):** هــي خدمة تقدم للمســتخدم قائمة بالمنظمات الموثوق بها والتي يمكن الاختيار من بينها للمصادقة.
- **هجمات رفض الخدمة الموزعة (Distributed denial-of-service attack):** هي عبارة عن اســتخدام العديد من الأنظمة المخترقة لإحداث رفض الخدمة لمستخدمي النظام المستهدف. ويشار إليها اختصاراً (DDoS).

- **مراقــب المجــال (Domain controller):** هو الخادم الــذي يُطبق قواعد الدليل النشط ضمن مجال محدد.
- **التشفير (Encryption):** هو الكتابة السرية للبيانات وتحويلها لإنتاج نص مشفر.
- **حمايــة نقطة النهاية (End point protection):** هي عبارة عن الأمن المُطبق في جهاز المُستخدم النهائي.
- **الأصول الضرورية (Essential asset):** هو الأصل الذي إذا تَسبب فقدان جاهزيته في عواقب وخيمة وفورية للمنظمة.
- **المراوغة (Evasion):** هي إجراء نشاط ضار بحيث يبدو أنه آمن.
- **الإيجابي الخاطئ (False positive):** هو الاكتشاف الذي يبدو أنه مشكلة (ايجابي) لكن عند إجراء المزيد من التحقيقات يتبين أنه ليس بمشكلة (أي يكون خاطئاً).
- **الرابطــة الاتحاديــة (federation):** هــي الرابطة التي تســد الفجــوة بين أنظمة المُصادقة في المنظمات المختلفة.
- **البيانــات الخاصــة بالارتبــاط الاتحــادي (Federation metadata):** هي عبارة عن مســتندات بـ «لغة الترميز الممتدة» (XML) تحتوي على قائمة شــاملة لأعضاء الارتباط الاتحادي، كما تحتوي على بيانات هامة مثل معلومات المنظمة ومعلومات التواصل وذلك لكل مزود خدمة ولكل مزود هوية.
- **مزود الارتباط الاتحادي (Federation provider):** هو الكيان المسؤول عن جميع المهام الإدارية المتعلقة بإدارة شؤون الاتحاد، مثل إدارة العضوية، وصياغة سياسات الارتباط وإنفاذها، وإدارة البنية التحتية للمفتاح العام اللازمة لعمليات التشفير.
- **الجُدُر النارية (Firewall):** هي شــكل من أشــكال الحماية التي تسمح لشبكة ما بالاتصال بشبكة أخرى مع الحفاظ على مستوى معين من الحماية.
- **النموذج (Framework):** هو هيكل لدعم شيء آخر.
- **الأصول العامة (General assets):** هي الأصول التي توجد في معظم المنظمات.

- **سياسـية المجموعـة (group policy):** هـي البنية التحتية التي تسـمح بتنفيذ ترتيبات محددة للمستخدمين والأجهزة.
- **دوال التجزئة (Hash functions):** هي طرق التشفير التي لا تستخدم مفاتيح.
- **الملفـات المخفيـة (Hidden files):** هي الملفات التي يتـم افتراضياً إخفاؤها عن المستخدمين.
- **الدليل الرئيسي (Home directory):** مكان المسـتخدم الخاص وهو مشابه لمجلد المستندات في نظام ويندوز. وهذا المصطلح شائع في أنظمة ينكس.
- **أنظمة كشف التسلل المعتمدة على المضيف (Host-based IDSs):** هي تطبيقات برمجيـة مُثبتة على المضيف الذي يراقب النشـاط الداخلي مثـل الوصول للملفات واسـتدعاء الأنظمة بهدف اكتشاف الأنشطة المشـبوهة. وأحياناً يتم اختصار هذا المصطلح على الشكل التالي (HIDSs).
- **القطع الاحتياطية السـاخنة (Hot spares):** هي المكونات الاحتياطية التي تستقر داخل الخادم وتَحِل محل الأجزاء المتعطلة دون حدوث أي تعطل في العمل.
- **تحديد الهوية (Identification):** هو عرض هوية المستخدم على النظام.
- **المُعرِف (Identifier):** هو عبارة عن سلسـلة من الأرقام التي تُعرِف بشـكل فريد الهوية في نظام السجلات.
- **الهوية (Identity):** هي سجل محدد محفوظ في نظام السجلات.
- **اثـراء الهويـة (Identity enrichment):** هـي جمع بيانات عـن علاقة كل فرد بالمنظمة.
- **إدارة الهوية (Identity management):** هي عمليات تحديد هوية الأفراد وجمع كافة البيانات اللازمة لمنح أو سحب امتيازات المستخدمين إلى الموارد.
- **مطابقـة الهويـة (Identity matching):** هـي عملية البحث في السـجل الحالي للشخص عن السجلات التي تتطابق مع مجموعة معينة من بيانات الهوية.

- **دمج الهوية (Identity merge):** هي دمج السجل الجديد أو المُحدث مع البيانات المرتبطة بالسجل الحالي للشخص.
- **ملاءمة الهوية (Identity reconciliation):** هي عملية مقارنة كل هوية مُكتشفة مع سجل رئيسي وذلك لجميع الأشخاص في المنظمة.
- **الأصول الذاتية (Idiosyncratic assets):** هي الأصول المميزة والخاصة للمنظمة.
- **سياسة الاستجابة للحوادث الأمنية (Incident response policy):** هي الطرق الموحدة المستخدمة من قبل المنظمة في التعامل مع حوادث أمن المعلومات.
- **الأصول المعلوماتية (Information asset):** هي المحتوى الإلكتروني المحفوظ والمملوك من قبل فرد أو منظمة.
- **أمن المعلومات (Information security):** هو حماية كل من المعلومات ونظم المعلومات من الأعمال غير المصرح بها كالوصول أو الاستخدام أو الإفشاء أو الإخلال أو التعديل أو التدمير وذلك لضمان التكامل، والخصوصية، والجاهزية.
- **ضوابط أمن المعلومات (Information security controls):** هي الضمانات المستخدمة للحد من آثار تهديدات أمن المعلومات.
- **نموذج أمن المعلومات (Information security model):** هو تمثيل للمكونات الأساسية لأمن المعلومات، ويوضح علاقة هذه المكونات مع بعضها البعض، ويستبعد النموذج أي شيء آخر.
- **الضوابط العامة لتقنية المعلومات (IT general controls):** هي أنشطة الرقابة التي تقوم بها تقنية المعلومات والتي تضمن المعالجة الصحيحة للمعاملات التجارية من قبل المنظمة.
- **مخاطر تقنية المعلومات (IT risk):** هي المخاطر المرتبطة باستخدام نظم المعلومات في المنظمة.
- **نظام تقنية المعلومات (IT system):** هو مجموعة من قطع أجهزة الحاسب الآلي والبرمجيات والبرامج الثابتة المهيأة لغرض معالجة وتخزين وإرسال المعلومات.

- **البنية التحتية كخدمة (Infrastructure as a Service):** هي نموذج أعمال تقوم المنظمات من خلاله باستخدام معدات وقطع الأجهزة كالمعالجات والتخزين وأجهزة التوجيه، وتعرف اختصاراً (IaaS).
- **الثغرات المتعلقة بالتحقق من صحة المدخلات (Input validation vulnerability):** هي الحالة التي يتم فيها استخدام مدخلات المُستخدِم في البرنامج دون التأكد من صحتها.
- **التثبيت (Installation):** هو كتابة البيانات اللازمة في المكان المناسب على القرص الصلب لجهاز الحاسب الآلي بهدف تشغيل البرنامج.
- **التكامل (Integrity):** هو الحماية من تعديل المعلومات أو تدميرها ويشمل ذلك التأكد من عدم إنكار المعلومات ومصداقية تلك المعلومات.
- **الملكية الفكرية (Intellectual property):** هي إبداعات العقل (الاختراعات والمصنفات الأدبية والفنية والرموز والأسماء والصور والتصاميم) والتي يمكن استخدامها لتحقيق الأرباح، ويشار إليها اختصاراً (IP).
- **الجدار الناري الداخلي (Interior firewall):** الأداة التي تُقيد الوصول لشبكة المنظمة الداخلية.
- **الوسطاء الداخليون (Internal agents):** هم الأشخاص الذين لهم صلة بالمنظمة وغالباً ما يكونون موظفين.
- **الشبكة الداخلية (Internal network):** هي موقع جميع الأصول المعلوماتية للمنظمة، ويطلق عليها أيضاً المنطقة المُسلحة.
- **أنظمة كشف التسلل (Intrusion detection systems):** هي مكونات مادية أو تطبيقات برمجية تراقب أنظمة تقنية المعلومات لاكتشاف الأنشطة الضارة أو اكتشاف انتهاكات سياسات الاستخدام التي أُنشئت من قبل مسؤول النظام. وتُعرف اختصاراً (IDS).

- **أنظمة منع التسلل (Intrusion prevention systems):** هي تقنيات يتم بناؤها على أنظمة كشف التسلل بهدف إيقاف الاختراقات المحتملة.
- **بروتوكول كيربيروس (Kerberos):** هو بروتوكول مصادقة يسمح للأجهزة الطرفية الموجودة في شبكة غير آمنة للتعريف بأنفسهم وللتعرف على بعضهم البعض، وذلك بشكل آمن باستخدام القطع الرمزية.
- **نواة نظام التشـغيل (Kernel):** البرنامج الذي يتحكم في مكونات الأجهزة، وإدارة الذاكرة، وتنفيذ التعليمات البرمجية على وحدة المعالجة المركزية، وإخفاء التفاصيل الضمنية لقطع الأجهزة من تطبيقات المستخدم.
- **مسـجل المفاتيح (Key loggers):** هو البرنامج الذي يتعقب ضربات مفاتيح لوحة المفاتيح في محاولة لجمع أسماء المستخدمين وكلمات المرور.
- **الأصـول القانونية المتعلقة بتقنية المعلومـات (IT-related legal assets):** هي التنظيمات التعاقدية التي توجه اسـتخدام أصول (مكونات الحاسـب الآلي المادية) والأصول البرمجية داخل المنظمة.
- **السجل (Logs):** هو سجلات لأداء جهاز الحاسب الآلي.
- **البرمجيـات الخبيثـة (Malware):** هـي البرمجيات أو الرمـوز المصممة خصيصاً لاستغلال جهاز الحاسب الآلي أو البيانات التي يحتويها دون موافقة المستخدم.
- **ثغرة الأذونات الناقصـة (Missing authorization vulnerability):** هي ثغرة تحدث عندما يسـمح البرنامج للمستخدمين بالوصول إلى أجزاء متميزة من البرنامج دون التحقق من بيانات اعتماد المستخدم.
- **بيـان الرسـالة (Mission statement):** هو تعبير قصـير (يُفضل أن يكون جملة واحدة أو جُملتين) عن خدمات المنظمة، والسوق المستهدف، والميزات التنافسية.
- **النموذج (Model):** هو تمثيل للعالم الحقيقي.
- **الرقابة (Monitoring):** هي الاستماع و/ أو تسجيل لأنشطة النظام بهدف الحفاظ على الأداء والأمن.

- **الاســتبدال الأحــادي الأبجــدي (Mono-alphabetic substitution):** هو نظام التشفير القائم على استبدال حروف منفردة بحروف أخرى بهدف التشفير.
- **معرفــة ما نحتاجه (Need-to-know):** هو مبــدأ لإدارة المعلومات يتم بناء عليه توفير المعلومات الضرورية فقط لأداء العمل.
- **الجُــدُر النارية للشــبكات (Network firewalls):** هي مكونات مادية أو برمجية تمنع الأخطار التي تنشأ في شبكة ما من الانتشار إلى شبكة أخرى.
- **أنظمة كشف التسلل المعتمدة على الشبكة (Network IDS):** هي أنظمة تراقب حركة مرور الشبكة ونشاط بروتوكول التطبيقات لتحديد الاتصالات المشبوهة.
- **بروتوكول (OAuth):** هو آلية تســمح للمســتخدم منح حــق الوصول من موارد خاصة في موقع ما (مزود الخدمة) إلى موقع آخر (العميل).
- **برمجيــات المصــدر المفتــوح (Open source software):** هــي البرمجيات التي يســتطيع أي شــخص أن يعدل في شــفرتها الأصلية ويقوم بنشر تعديلاته في جميع أنحاء العالم.
- **المسؤوليات التشــغيلية (Operational responsibilities):** هي مسؤولية الفرد أو الوحدة عن وظيفة محددة تتعلق باستخدام أحد الأصول.
- **أنظمــة التشــغيل (Operating systems):** هي برمجيــات تدير مكونات أجهزة الحاسب الآلي وتوفر الخدمات العامة لتطبيقات المستخدم.
- **تحديــث البرمجيــات (Operating system updates):** هو اســتبدال المكونات المعيبة للبرامج بمكونات أخرى خالية من تلك العيوب التي تم تحديدها.
- **الجُــدُر النارية لتصفية الحُزم (Packet filtering firewalls):** الجُدر النارية التي تقــوم بفحص الحقول العلوية لبروتوكول الحزم التي تتدفق من خلال الجدار الناري لتحديد ما إذا كان سيُسمح للحزمة بالدخول للشبكة.
- **تحسس رزم البيانات (Packet sniffing):** وهو عبارة عن القيام باعتراض ومراقبة البيانات التي تمر عبر شبكة أجهزة الحاسب الآلي.

- **الدليــل الأم (Parent Directory):** هــو الدليل (المجلد) الــذي يأتي مباشرة بعد الدليل الحالي في التسلسل الهرمي.
- **الشركاء (Partners):** وهم أي طرف ثالث يتقاسم علاقة العمل مع المنظمة.
- **عبارة المرور (Passphrase):** هي سلسلة من الكلمات التي تمثل كلمة السر.
- **كلمــة المرور (Password):** هي سلســلة من الرموز السرية التي لا يعرفها ســوى صاحب الهوية ويقوم باستخدامها للمصادقة على الهوية.
- **التقاط كلمة المرور (Password capturing):** هو قدرة أحد المهاجمين على الحصول على كلمة المرور من مكان حفظها، أو أثناء إرسالها، أو من معرفة المستخدم وسلوكه.
- **كسر كلمات المرور (Password cracking):** هو عملية توليد سلســلة من الرموز التي تطابق أي سلسلة من سلاسل كلمات المرور الموجودة على النظام المستهدف.
- **انتهاء صلاحية كلمة المرور (Password expiration):** هو تحديد المدة التي يمكن خلالها استخدام كلمة المرور قبل أن يكون مطلوب من المستخدم أن يقوم بتغييرها.
- **تخمــين كلمات المــرور (Password guessing):** القيــام المتكرر بتجريب كلمات مــرور مختلفة، مثل كلمات المرور الافتراضية وكلــمات القاموس، إلى أن يتم العثور على كلمة المرور الصحيحة.
- **إدارة كلمات المــرور (Password management):** هي عبارة عن عملية تحديد سياسات كلمات المرور وتنفيذها والحفاظ عليها في جميع أنحاء المنظمة.
- **سياســات كلمات المــرور (Password policy):** هي مجموعــة من القواعد ذات العلاقة باستخدام كلمات المرور.
- **اســتبدال كلمة المرور (Password replacing):** هو استبدال كلمة المرور الحالية للمستخدم بكلمة مرور أخرى لا يعرفها إلا المهاجم.
- **مزامنــة كلمات المــرور (Password synchronization):** هي خدمة لضمان أن المستخدم لديه نفس اسم المستخدم وكلمة المرور في جميع الأنظمة.

- **التصحيح (Patch):** هو برنامج يعمل على تصحيح المشكلات الأمنية والوظيفية في البرمجيات والبرامج الثابتة.
- **إدارة التصحيحــات (Patch management):** هــي عمليــة تحديد التصحيحات والحصول عليها وتثبيتها والتحقق منها.
- **محيــط الجدار الناري (Perimeter firewall):** هــو جدار الحماية الذي يقع بين الشبكة الخارجية والمنظمة.
- **الشــبكة المحيطة (perimeter network):** هي الشــبكة التي تقع بين الشــبكة الخارجية والشبكة الداخلية للمنظمة. وتقوم الشبكة المحيطة باستضافة الخدمات الخارجيــة مثــل بروتوكول انتقال النص التشــعبي (http)، وبروتوكــول نقل البريد الإلكتروني (smtp)، ونظام اســم المجال (DNS). وتســمى أيضــاً المنطقة منزوعة السلاح.
- **الإحلال (Permutation):** هو تحديد مكان المخرجات لكل ١٠٠٠ بت من المدخلات.
- **سجل الشخص (Person Registry):** هو المحور المركزي الذي يربط المُعرِفات من جميع نظم الســجلات في هوية رئيســية واحدة، ويجعل من ارتباط وانتقال بيانات الهوية (مثل الرقم الجامعي والرقم الوظيفي) أمراً ممكناً.
- **إنشــاء الهويــة (Identity creation):** الوظيفة التي تقوم بإنشــاء ســجل جديد ومُعرِف جديد تابع له ويكون ذلك في سجل الشخص.
- **رقم التعريف الشــخصي (Personal identification number):** هو كلمة مرور عددية قصيرة تتكون من ٤ إلى ٦ أرقام. ويشار إليه اختصاراً (PIN).
- **الانتحــال (Phishing):** هو محاولة اختراق مســتخدم ما عن طريق التنكر كجهة موثوق بها في التواصل الإلكتروني.
- **الضوابــط الماديــة (Physical controls):** وهي عبارة عن اســتخدام الأســاليب التقليدية غير التقنية لمنع الضرر.

- **السياسات (Policy):** هي وثيقة تُسجل مبادئ رفيعة المستوى أو مسار العمل الذي تم إقراره.
- **المراقبة الاستباقية (Proactive testing):** هي فحص النظام لمشكلات محددة قبل حدوثها.
- **الضوابط الإجرائية (Procedural controls):** هي عبارة عن خطط محددة للإجراءات التي تتحكم في استخدام موارد أجهزة الحاسب الآلي.
- **الثغرات الإجرائية (Procedural vulnerability):** هي عبارة عن ضعف في الطُرق التشغيلية للمنظمة والتي يمكن استغلالها لانتهاك السياسة الأمنية.
- **أنظمة كشف التسلل المُعتمدة على حالات البروتوكول (Protocol-state-based IDS):** هي أنظمة كشف تسلل تقوم بمقارنة الأحداث المُلاحظة بنشاط البروتوكول المُحدد، وذلك لكل حالة بروتوكول بهدف تحديد الانحرافات.
- **التشفير بالمفتاح العام (Public-key cryptography):** هو طرق التشفير التي تستخدم مفتاحين أحدهما للتشفير والآخر لفك التشفير.
- **المراقبة التفاعلية (Reactive monitoring):** هي كشف وتحليل حالات الفشل بعد حدوثها.
- **التكرارية (Recursion):** هي تحديد وظيفة اعتماداً على ما تقوم به تلك الوظيفة.
- **توفير القطع الاحتياطية (Redundancy):** هو توفير إمكانيات إضافية يتم المحافظة عليها لتحسين موثوقية النظام.
- **حماية نقطة النهاية المُعتمدة على الشهرة (Reputation-based end point protection):** هي تَنبؤ أمان الملف اعتماداً على نقاط الشهرة التي يتم حسابها بواسطة خواص الملف الملحوظة.
- **الأصول المطلوبة (Required asset):** هي الأصول المهمة للمنظمة وفي الوقت نفسه تكون المنظمة قادرة على الاستمرار في العمل لفترة من الوقت حتى إذا كانت تلك الأصول غير موجودة.

- **الأصـــول المقيـــدة (Restricted asset):** هي الأصول التي يــؤدي الإفصاح عنها أو تغييرها إلى عواقب وخيمة على المنظمة.
- **المخاطر (Risk):** هي مقياس كمي للضرر المحتمل من التهديد.
- **تقييم المخاطــر (Risk assessment):** تحديد جميع المخاطر التي تواجه المنظمة وتجميعها.
- **إطار المخاطر (Risk frame):** يوضح البيئة التي تُتخذ فيها القرارات المعتمدة على المخاطر، ويساعد على تأسيس سياق إدارة المخاطر.
- **إدارة المخاطر (Risk management):** هي إدارة التأثيرات المالية للأحداث غير العادية.
- **مراقبــة المخاطــر (Risk monitoring):** هي تقييم فاعلية خطــة إدارة المخاطر للمنظمة مع مرور الوقت.
- **الاســتجابة للمخاطر (Risk response):** هي كيفية اســتجابة المنظمات للمخاطر بمجرد تحديدها بواسطة تقييم المخاطر.
- **دور الفرد (Role):** هي علاقة الفرد بالمنظمة، ويشار لها أيضاً بالانتماء للمنظمة.
- **نظام التحكم في الوصول المُعتمِد على الدور (Role-based access control):** هو نظــام يمنح الأفراد ذوي الأدوار المحددة امتيازات وصول تتناســب مع أدوار النظام المناظرة لها. ويشــار لها اختصاراً (RBAC)، ويقوم بتعيين أذونات لدور المستخدم بدلاً من تعيين أذونات للمستخدم الفردي.
- **تقنية التحكم الخفي في جهاز الحاسب الآلي (Rootkits):** هي عبارة عن مجموعة من البرمجيات تُستخدم لإخفاء وجود البرامج الضارة في نظام الحاسب الآلي.
- **النطاق (Scope):** هو جزء من سياســة الاستجابة للحوادث الأمنية ويقوم بتحديد أهداف هذه السياسة.
- **التشــفير بالمفتاح السري (Secret key cryptography):** هي طرق التشفير التي تستخدم مفتاحاً واحداً لكل من التشفير وفك التشفير.

- **فصل المهام (Separation of duties):** هي الحالة التي يقوم فيها أكثر من شخص بإتمام مهمة كاملة.
- **اتفاقيــة مســتوى الخدمــة (Service Level Agreement):** هي وثيقة تحدد ما الــذي تقوم به وحــدة تقنية المعلومات وكيــف تقوم بذلك، وذلــك لإنجاز وإدارة توقعات العميل أو مالك النظام.
- **القشرة (shell):** هي برنامج نصي يسمح للمستخدم بالتفاعل مباشرة مع نواة نظام التشغيل.
- **تطبيقــات بروتوكول (Shibboleth):** هي تطبيقات لإدارة الهوية مفتوحة المصدر وذات بنية تحتية للتحكم بوصــول الارتباط الاتحادي ومعتمدة على برتوكول «لغة تمييز التأكيدات الأمنية» (Security Assertion Markup Language)، والمعروفة اختصاراً (SAML).
- **التوقيع (Signature):** هو سلســلة من البايتــات المعروف عنها أنها جزء من البرمجيات الضارة.
- **نقطة العطل المفردة (Single point of failure):** هي جزء من النظام إذا تعطل يؤدي إلى توقف النظام بأكمله.
- **تســجيل الدخول الأحادي (Single sign-on):** هو التقنية التي تسمح للمستخدم بتســجيل الدخول مرة واحدة ومن ثم الوصول إلى جميع الموارد المُصرح للمستخدم الوصول لها.
- **الهندســة الاجتماعية (social engineering):** وهي فــن التلاعب بالناس بهدف تنفيذ المهام المطلوبة.
- **البرمجيات كخدمة (Software as a Service):** وهي آلية لتســليم البرمجيات يتم فيهــا توفير التطبيقات وجميــع الموارد المرتبطة بها إلى المنظــمات عن طريق مُورِد البرمجيات كخدمة وتتم من خلال متصفح الإنترنت. ويشار إليها اختصار (SaaS).

- **الأصـول البرمجيـة (Software assets):** هـي الأدوات البرمجيـة اللازمة لمعالجة معلومات المنظمة بهدف تحقيق رسالة المنظمة.
- **تحديـث البرمجيـات (Software update):** هو التحديث الذي يُصلح مشـكلات المكونات المنخفضة المستوى لبرمجيات النظام، ويتم تطويرها وإصدارها مباشرة من مُورِد النظام.
- **الثغرات البرمجية (Software vulnerability):** هي أخطاء في مواصفات أو تطوير أو ضبط البرمجيات بحيث ينتهك تنفيذ تلك البرمجيات سياسة الأمان.
- **ثغرات حقن اللغة الاستفسارية الإنشائية المركبة (SQL injection vulnerability):** ويقصد بها استخدام مدخلات لغة الـ (SQL) غير المُتَحَقق منها في التطبيقات.
- **المعيار (Standard):** هو مجموعة محددة من القواعد المقبولة والمعتمدة من قبل العديد من المنظمات.
- **إخفاء المعلومات (Steganography):** وهو إخفاء المعلومات بطريقة لا يشك أحد في وجودها.
- **الاسـتبدال (Substitution):** هو تحديد مخرجات ١٠٠٠ بت (k-bit) لكل ١٠٠٠ بت (k-bit) من المدخلات.
- **إدارة الأنظمـة (System administration):** هي مجموعـة من الوظائف التي توفر خدمات الدعم، وتضمن الثقة في العمليات، وتعزز الاسـتخدام الفعال للنظام، وتضمن تحقيق أهداف جودة الخدمة المحددة.
- **مسـؤول النظام (System administrator):** هو الشخص المسؤول عن العمليات اليومية للأنظمة التقنية.
- **نظام السـجلات (System of Record):** هو النظام الذي يحتوي السـجلات التي يمكن من خلالها اسـترداد المعلومات بالاسـم، أو رقم الهوية، أو الرمز، أو أي مُعرِف مُحدد على وجه الخصوص للفرد. ويشار إليه أحياناً (SOR).

- **التحديــد النمطي لمواصفات النظام (System profiling):** هو تجميع كل الأصول التي تم جردها، وتصنيفها حسب الوظيفة، وفهم الاعتمادية بين تلك الأصول.
- **مسؤول أمن النظام (System security officer):** هو الشخص المسؤول عن وضع وتطبيق ومراجعة إجراءات الأمن التشغيلية في المنظمة.
- **الضوابــط التقنيــة (Technical controls):** وهــي عبارة عن الإجــراءات الأمنية المبنية في نظم المعلومات نفسها.
- **التهديدات (Threat):** هي القدرات والنوايا وأساليب الهجوم من الأعداء لاستغلال أو الإضرار بالأصول.
- **وســيط التهديد (Threat agent):** هو فرد أو منظمة أو مجموعة تقوم بتأســيس نشاط تهديد معين.
- **نموذج التهديد (Threat model):** هو التفاعل بين الوســطاء والأنشــطة والأصول الذي يواجه المنظمة.
- **القطع الرمزية (Tokens):** هي المكونات المادية (أو في حالة القطع الرمزية البرمجية المخزنة في شيء مادي) التي يجب تقديمها لإثبات هوية المستخدم.
- **ثغرة البيانــات غير المشــفرة (Unencrypted data vulnerability):** هي ثغرة تحــدث عندما يتم تخزين بيانات حساســة محلياً أو عندما يتم نقلها عبر الشــبكة بدون التشفير السليم.
- **الأصول غير المقيدة (Unrestricted assets):** هي الأصول التي تختلف عن الأصول التي تُصنف بأنها مقيدة. وهي البيانات التي إذا سُربت أو تم اســتعراضها من قبل شخص ما لن يسبب ذلك مشكلات للمنظمة.
- **ثغرة رفع الملفات غير المقيــد (Unrestricted uploads vulnerability):** وهي ثغــرة تحدث عندما يتم قبول الملفات من قبل البرمجيات دون التأكد من أن الملف يتبع مواصفات دقيقة.

- **إدارة المســتخدم (User management):** هي تحديد حقوق أعضاء المنظمة فيما يتعلق بالمعلومات الموجودة في المنظمة.
- **الفيروسات والدودة الحاسوبية (Viruses and worms):** هي برمجيات تؤثر سلباً في أجهزة الحاسب الآلي وتنتشر من خلال الشبكة دون موافقة المستخدم.
- **بيان الرؤية (Vision statement):** هو بيان يقوم بالإفصاح عن تطلعات المنظمة.
- **الثغرات (Vulnerability):** هي نقاط ضعف في أمن المعلومات تعطي التهديدات الفرصة بأن تصبح خطراً على الأصول.
- **المزج من محتويات الشبكة الأخرى (web mashups):** هو عبارة عن صفحة ويب أو تطبيق تقدم خدمة جديدة من خلال دمج بيانات واحد أو أكثر من واجهة برمجة التطبيقات (API) على الإنترنت.
- **الاســتغلال الفوري (zero-day exploits):** هو تهديد يتم من خلاله اختراق ثغرة لم تكن معروفة في برمجيات الحاسب الآلي.
- **الزومبي (Zombie):** وهو جهاز حاســب آلي متصــل بالإنترنت تم اختراقه لتنفيذ المهام الضارة بتوجيه من مُتحكِم عن بعد.
- **عملاء الزومبي (zombie clients):** هو برنامج يتلقى الأوامر من جهاز حاسب آلي عن بعد ويســتخدم جهاز الحاســب المُصاب لأداء مهام ضارة وفقاً للتوجيهات التي يتلقاها.

كشّاف موضوعات الكتاب

المترجم في سطور

د. جعفر بن أحمد عبدالكريم العلوان

المؤهل العلمي:

- دكتوراه في إدارة الأعمال - نظم معلومات - جامعة فرجينيا كومونويلث بالولايات المتحدة الأمريكية.

الوظيفة الحالية:

- أستاذ إدارة الأعمال المشارك ومدير إدارة البحوث والاستشارات بفرع معهد الإدارة العامة بالمنطقة الشرقية.

أبرز الأعمال العلمية المنشورة والمقبولة للنشر في مجلات عربية:

- تكنولوجيا الجيل الثاني للحكومة الإلكترونية وعلاقتها بشفافية المعلومات ورضا الموظفين عن العملية الإدارية: دراسة وصفية تحليلية في الأجهزة الحكومية السعودية، المجلة العربية للإدارة (مقبول للنشر).
- أثر استخدام تكنولوجيا الجيل الثاني للحكومة الإلكترونية على القدرات الإبداعية لموظفي الأجهزة الحكومية بمدينة الدمام بالمملكة العربية السعودية، مجلة جامعة الإمام محمد بن سعود للعلوم الإنسانية والاجتماعية (مقبول للنشر).
- الاتجاهات الإدارية المعاصرة في تنمية الموارد البشرية: مراجعة منهجية للأدبيات ذات العلاقة، مجلة جامعة الإمام محمد بن سعود للعلوم الإنسانية والاجتماعية (مقبول للنشر).
- معوقات التخطيط الإستراتيجي في مؤسسات العمل الخيري: دراسة ميدانية على الجمعيات الخيرية في المملكة العربية السعودية، مجلة جامعة الملك عبدالعزيز للاقتصاد والإدارة، (٢٠١٧)، عدد ٢، مجلد ٣٢.

- عوامل الفساد الإداري في الأجهزة الحكومية السعودية من وجهة نظر موظفي القطاع الحكومي، مجلة جامعة الملك عبدالعزيز للاقتصاد والإدارة، (٢٠١٦)، عدد ١، مجلد ٣٠.
- العوامل المؤثرة على أنظمة الموارد البشرية الإلكترونية: دراسة ميدانية على منظمات القطاع الخاص في المملكة العربية السعودية، المجلة العربية للإدارة، (٢٠١٥)، عدد ١، مجلد ٣٥.
- نموذج مقترح لتقييم نظام التعليم عن بعد في جامعة الملك فيصل بالمملكة العربية السعودية، مجلة العلوم الإنسانية والإدارية التابعة لجامعة الملك فيصل، (٢٠١٤)، عدد ٢، مجلد ١٥.

أبرز الأعمال العلمية المعروضة في مؤتمرات عربية:

- الشفافية والمساءلة في مستشفيات وزارة الصحة بالمملكة العربية السعودية، المؤتمر العلمي الثالث لكليات الاقتصاد والإدارة بعنوان الاقتصاد الوطني التحديات والطموح، (٢٠١٦)، جامعة الملك عبدالعزيز، جدة.
- رضا المستفيد عن خدمات مؤسسات العمل الخيري بالمملكة العربية السعودية، مؤتمر التنمية الإدارية الواقع والطموح، (٢٠١٦)، جامعة الجوف، الجوف (عمل مشترك مع أ. عبدالله إبراهيم الدرازي).
- الحكومة الذكية ودورها في تطوير خدمات الأجهزة الحكومية، مؤتمر ثقافة خدمة العملاء في القطاع الحكومي، (٢٠١٥)، معهد الإدارة العامة، الرياض.
- التقييم الشامل والمستمر لنظام التعلم عن بعد، المؤتمر الدولي الثالث للتعلم الإلكتروني والتعليم عن بعد: الممارسة والأداء المنشود، (٢٠١٣)، الرياض.
- دور أنظمة الحكومة الإلكترونية في مكافحة الفساد الإداري: حالة من الحكومة الإلكترونية القطرية، مؤتمر التنمية الإدارية في دول مجلس التعاون لدول الخليج العربية: تحديات التغيير والتطوير واستشراف المستقبل، (٢٠١٢)، معهد الإدارة العامة، الرياض.

أبرز الأعمال العلمية المنشورة في مجلات أجنبية:

- Thomas, M., Alalwan, J. Designing a Semantic Tool to Evaluate Web Content of Government Websites, (2017) International Journal of Public Administration in the Digital Age, 3, 2, 19- 36
- Alalwan, J. Thomas, M. Weistroffer, H. Decision Support Capabilities of Enterprise Content Management Systems: An Empirical Investigation, (2014) Decision Support Systems, 68, 39 -48
- Alalwan, J. Continuance Intention to Use Government 2.0 Services: The Impact of Citizens' Satisfaction and Involvement, (2013), International Journal of Electronic Government Research, 9, 3, 58- 74
- Alalwan, J. A Taxonomy for Decision Support Capabilities of Enterprise Content Management Systems, (2013), Journal of High Technology Management Research, 24, 1, 10 -17
- Alalwan, J. and Weistroffer, H.R Enterprise Content Management Research: A Comprehensive Review, (2012), Journal of Enterprise Information Management, 25, 5, pp. 441 -461
- Alalwan, J. and Thomas, M. A. An Ontology-based Approach to Assessing Records Management Systems, (2012), eService Journal, 8, 3, 24 -41
- Alalwan, J. IT Resources and the Strategic Conditions to Maintain Sustainable Competitive Advantage (2012), International Journal of Information, Business and Management, 4, 2, 46 -54

أبرز الدراسات المعروضة في مؤتمرات أجنبية:

- Alalwan, J. Managerial Crisis Information Systems Model: Key Success Factors of Crisis Information Systems, (2017) International Conference on Business and Economics Studies, Houston, USA
- Alalwan, J. Harnessing E-Governance Initiatives: Building Competence Organizations, (2016) Los Angeles International Business and Social Science Research Conference, California, USA
- Alalwan, J. Recruiters' Intention to Adopt Social Information Systems, (2014) In Proceedings of the Americas Conference on Information Systems, Savannah, USA
- Alalwan, J. The Exploitation of the Action Research Accumulated Knowledge: Analogical Reasoning Perspective, (2014), 7th IADIS International Conference on Information Systems, Madrid, Spain
- Alalwan, J. Continuance Intention to Use Government 2.0 Services: A Theoretical Study, (2013), International Research Conference on E-Business Management, Dubai, UAE
- Alalwan, J. and Weistroffer, H.R. Strategic Information Systems Planning in Saudi Arabian Educational Institutions (2012), In Proceedings of the Southern Association for Information Systems, Atlanta, USA
- Alalwan, J. Decision Support and Enterprise Content Management Systems: Current and Future Trends (2012), In Proceedings of the Southeast Decision Sciences Institute, pp. 702 -709

- Alalwan, J. Influence of Trust, Security, and Privacy on IS Continuance Intention: A Theoretical Model (2012), In Proceedings of the Southeast Decision Sciences Institute, pp. 158- 165
- Alalwan, J. and Thomas, M. A. A Holistic Framework to Evaluate E-government Systems (2011), In Proceedings of the Americas Conference on Information Systems, Michigan, USA
- Alalwan, J. and Weistroffer, H.R. Decision Support Capabilities of Enterprise Content Management: A Framework (2011), In Proceedings of the Southern Association for Information Systems, Atlanta, USA
- Alalwan, J. and Thomas, M.A. Designing ERM Ontology to Evaluate Records Management - System (2011), In Proceedings of the Hawaii International Conference on Systems Sciences, USA



مراجع الترجمة في سطور

أ. د. عبدالله بن عبدالعزيز بن عبدالله التميم

المؤهل العلمي:

- دكتوراه في علوم الحاسب الآلي ونظم المعلومات، جامعة برادفورد - بريطانيا.

المؤهلات العملية:

- أستاذ دكتور بكلية علوم الحاسب والمعلومات بجامعة الإمام محمد بن سعود الإسلامية.
- عميد سابق لكلية علوم الحاسب والمعلومات وكلية العلوم بجامعة الإمام.
- مدير برنامج أبحاث تقنية المعلومات المدعوم من مدينة الملك عبدالعزيز للعلوم والتقنية.
- شارك في عضوية عدد من اللجان والمجالس داخل وخارج الجامعة. كما شارك في عضوية لجان علمية وفنية لأكثر من ثلاثين مؤتمراً عالمياً.
- له أكثر من خمسين ورقة علمية في مجلات ومؤتمرات علمية عالمية.
- محكم خارجي لعدد من الجامعات داخل وخارج المملكة.
- له خبرات استشارية في العديد من القطاعات الحكومية والخاصة.
- حاصل على عدد من جوائز التفوق والإنجاز ومنها جائزة القائد النموذجي في قارة آسيا في القطاع الأكاديمي، وذلك خلال حفل جوائز القيادات الآسيوية ٢٠١٢ الذي أقيم في دبي.

تم التصميم والإخراج الفني والطباعة في
الإدارة العامة للطباعة والنشر بمعهد الإدارة العامة - ١٤٤٠هـ

هذا الكتاب

إن مشكلات أمن المعلومات مزعجة ومُكلِفة ومُستمرة بما فيه الكفاية، لتجعل من أمن المعلومات مهنة العصر الحديث وتجعل منه كذلك موضوعاً جديراً بالاهتمام والدراسة؛ لذا تم تصميم هذا الكتاب ليكون بمثابة مقرر دراسي مخصص لأمن المعلومات تتم دراسته خلال فصل دراسي واحد. ويركز الكتاب على مساعدة الطلاب على اكتساب المهارات المطلوبة في سوق العمل المهنية. ويبدأ الكتاب بمقدمة عن البيئة المهنية لأمن المعلومات. وبعد اقتناع الطالب بأهمية هذا الموضوع، يُقدّم الكتاب النموذج الأساسي لأمن المعلومات والذي يتكون من الأصول، والثغرات الأمنية، والتهديدات، والضوابط. وما تبقى من الكتاب يستعرض مفاهيم توصيف الأصول، والثغرات الأمنية، والتهديدات والاستجابة لها باستخدام التحكم الأمني. وينتهي الكتاب بدمج هذه الموضوعات تحت المظلة العامة لإدارة المخاطر التنظيمية. وبنهاية المقرر الدراسي سيكون الطالب ملماً بكيفية تطور الاهتمام بأمن المعلومات في المجتمع، وكيفية استخدام الأطر والنماذج الحديثة للتعامل مع تلك المخاوف في بيئة احترافية.



تصميم وإخراج وطباعة الإدارة العامة للطباعة والنشر ـ معهد الإدارة العامة ١٤٤٠هـ